

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Kenichi TAKEDA, et al.

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: PRINTER DRIVER PROGRAM AND PRINTER

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2003-078788	March 20, 2003

Certified copies of the corresponding Convention Application(s)

☒ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number

Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

Customer Number

22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

C. Irvin McClelland  
Registration Number 21,124

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2003年 3月20日

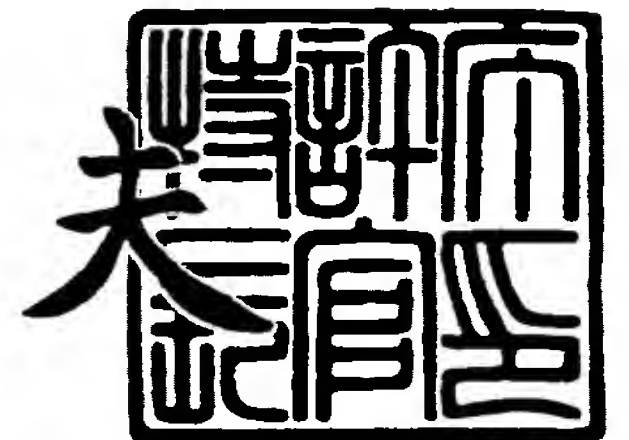
出 願 番 号  
Application Number: 特願2003-078788  
[ST. 10/C]: [JP2003-078788]

出 願 人  
Applicant(s): 株式会社リコー

2003年11月10日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0301447

【提出日】 平成15年 3月20日

【あて先】 特許庁長官殿

【国際特許分類】 B41J 29/38  
G06F 3/12

【発明の名称】 プリンタドライバプログラムおよびプリンタ装置

【請求項の数】 22

【発明者】

    【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

    【氏名】 武田 健一

【発明者】

    【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

    【氏名】 西脇 浩文

【発明者】

    【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

    【氏名】 澤田 のぞみ

【発明者】

    【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

    【氏名】 大谷 正樹

【特許出願人】

    【識別番号】 000006747

    【氏名又は名称】 株式会社リコー

【代理人】

    【識別番号】 100089118

    【弁理士】

    【氏名又は名称】 酒井 宏明

【手数料の表示】

【予納台帳番号】 036711

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9808514

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 プリントドライバプログラムおよびプリンタ装置

【特許請求の範囲】

【請求項 1】 ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリントドライバプログラムであって、

所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、

前記暗号化されたアプリ文書データと前記文書認証情報処理手順によって入力された文書認証情報とを含む印刷データを生成する印刷データ生成手順と、

前記印刷データ生成手段によって生成された印刷データをネットワークに接続されたプリンタ装置に送信する送信手順と、

をコンピュータに実行させるプリントドライバプログラム。

【請求項 2】 ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリントドライバプログラムであって、

前記プリンタ装置との間で予め定められた第 1 の鍵情報を前記プリンタ装置から取得して、第 1 の鍵情報に基づいて第 2 の鍵情報を生成する鍵生成手順と、

所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、

前記文書認証情報処理手段によって入力された前記文書認証情報と前記暗号化されたアプリ文書データとを含む印刷データを生成する印刷データ生成手順と、

前記鍵生成手段によって生成された第 2 の鍵情報によって前記印刷データを暗号化する暗号化手順と、

前記暗号化手段によって暗号化された印刷データと前記第 2 の鍵情報を、ネットワークに接続されたプリンタ装置に送信する送信手順と、

をコンピュータに実行させるプリントドライバプログラム。

【請求項 3】 前記第 1 の鍵情報を前記プリンタ装置に要求する要求手順をさらにコンピュータに実行させる請求項 2 に記載のプリントドライバプログラム。

【請求項 4】 ネットワークに接続された時点で、接続通知を前記プリンタ

装置に送信し、前記接続通知の送信後に、前記プリンタ装置から前記第 1 の鍵情報を受信する受信手順をさらにコンピュータに実行させる請求項 2 に記載のプリンタドライバプログラム。

【請求項 5】 ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラムであって、

所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、

前記文書認証情報処理手順によって入力された前記文書認証情報と前記暗号化されたアプリ文書データとを含む印刷データを生成する印刷データ生成手順と、

プリンタ装置から取得した公開鍵情報によって前記印刷データを暗号化する暗号化手順と、

前記暗号化手順によって暗号化された印刷データとクライアント装置に固有の識別情報を、ネットワークに接続されたプリンタ装置に送信する送信手順と、

をコンピュータに実行させるプリンタドライバプログラム。

【請求項 6】 前記公開鍵情報を前記プリンタ装置に要求する要求手順をさらにコンピュータに実行させる請求項 5 に記載のプリンタドライバプログラム。

【請求項 7】 ネットワークに接続された時点で、接続通知を前記プリンタ装置に送信し、前記接続通知を送信後に、前記プリンタ装置から前記公開鍵情報を受信する受信手順をさらにコンピュータに実行させる請求項 5 に記載のプリンタドライバプログラム。

【請求項 8】 印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させるジョブ認証情報処理手順をさらにコンピュータに実行させ、

前記印刷データ生成手順は、さらに前記ジョブ認証情報処理手順によって入力された前記ジョブ認証情報を含む前記印刷データを生成することを特徴とする請求項 2 ～ 7 のいずれか一つに記載のプリンタドライバプログラム。

【請求項 9】 前記文書認証情報処理手段によって入力された文書認証情報から印刷ジョブを開始させるためのジョブ認証情報を生成するジョブ認証情報処理手順をさらにコンピュータに実行させ、

前記印刷データ生成手順は、さらに前記ジョブ認証情報処理手順によって生成

された前記ジョブ認証情報を含む前記印刷データを生成することを特徴とする請求項 2 ～ 7 のいずれか一つに記載のプリンタドライバプログラム。

【請求項 1 0】 前記ジョブ認証情報処理手順は、前記文書認証情報処理手段によって入力された文書認証情報と同一データを前記ジョブ認証情報として生成することを特徴とする請求項 9 に記載のプリンタドライバプログラム。

【請求項 1 1】 ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、

前記クライアント装置から受信した印刷データに含まれる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、

前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、

を備えたことを特徴とするプリンタ装置。

【請求項 1 2】 ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、

前記クライアント装置との間で予め定められた第 1 の鍵情報を生成し、生成された前記第 1 の鍵情報を前記クライアント装置に送信する第 1 の鍵情報生成手段と、

前記クライアント装置から受信した前記第 1 の鍵情報に関連する第 2 の鍵情報から前記第 1 の鍵情報を生成するとともに、前記クライアント装置から受信した印刷データを、前記第 1 の鍵情報によって復号化する復号化手段と、

前記印刷データに含まれる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、

前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、

を備えたことを特徴とするプリンタ装置。

【請求項 1 3】 前記第 1 の鍵生成手段は、前記クライアント装置から前記第 1 の鍵情報の要求を受信した場合に、前記第 1 の鍵情報を生成し、生成された前記第 1 の鍵情報を、直ちに要求のあった前記クライアント装置に送信することを特徴とする請求項 1 2 に記載のプリンタ装置。



【請求項 14】 前記第 1 の鍵生成手段は、前記クライアント装置から前記第 1 の鍵情報の要求を受信した場合に、前記第 1 の鍵情報を生成し、生成された前記第 1 の鍵情報を、印刷可能な状態となった時点で要求のあった前記クライアント装置に送信することを特徴とする請求項 12 に記載のプリンタ装置。

【請求項 15】 前記第 1 の鍵生成手段は、前記第 1 の鍵情報を生成し、前記クライアント装置がネットワークに接続された時点で前記クライアント装置に送信することを特徴とする請求項 12 に記載のプリンタ装置。

【請求項 16】 前記復号化手段は、前記クライアント装置から前記第 2 の鍵情報を受信した場合に、前記第 1 の鍵情報生成手段によって生成された前記第 1 の鍵情報と、受信した第 2 の鍵情報から生成された第 1 の鍵情報とを比較し、両第 1 の鍵情報が一致する場合にのみ前記印刷データの復号化を行うことを特徴とする請求項 12 ～ 15 のいずれか一つに記載のプリンタ装置。

【請求項 17】 ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、

クライアント装置に固有の識別情報に対する秘密鍵情報から公開鍵情報を生成し、クライアント装置に送信する公開鍵処理手段と、

前記クライアント装置から受信した印刷データを、前記クライアント装置から受信した識別情報に対応する秘密鍵情報によって復号化する復号化手段と、

前記印刷データに含まれる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、

前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、

を備えたことを特徴とするプリンタ装置。

【請求項 18】 前記クライアント装置から前記公開鍵情報の要求を受信した場合に、前記秘密鍵情報を生成する秘密鍵生成手段と、

前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を直ちに前記クライアント装置に送信する公開鍵処理手段と、

をさらに備えたことを特徴とする請求項 17 に記載のプリンタ装置。



【請求項 1 9】 前記クライアント装置から前記公開鍵情報の要求を受信した場合に、前記秘密鍵情報を生成する秘密鍵生成手段と、

前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を、印刷可能な状態になった時点で前記クライアント装置に送信する公開鍵処理手段と、

をさらに備えたことを特徴とする請求項 1 7 に記載のプリンタ装置。

【請求項 2 0】 前記クライアント装置に対する前記秘密鍵情報を生成する秘密鍵生成手段と、

前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を、前記クライアント装置がネットワークに接続された時点で前記クライアント装置に送信する公開鍵処理手段と、

をさらに備えたことを特徴とする請求項 1 7 に記載のプリンタ装置。

【請求項 2 1】 前記クライアント装置の識別情報と前記秘密鍵情報と前記秘密鍵情報の有効期間とを対応付けた鍵管理情報を記憶する記憶手段をさらに備え、

前記復号化手段は、前記クライアント装置から前記クライアント情報を受信した場合に、前記鍵管理情報を参照して、前記クライアント情報に対応する前記秘密鍵情報が前記有効期限の範囲内にあるか否かを判断し、前記有効期限の範囲内にある場合にのみ前記印刷データを復号化することを特徴とする請求項 1 7 ～ 2 0 のいずれか一つに記載のプリンタ装置。

【請求項 2 2】 前記復号化手段は、印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させ、前記印刷データを復号化することを特徴とする請求項 1 2 ～ 2 0 のいずれか一つに記載のプリンタ装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、暗号化されたアプリケーションの文書をプリンタ装置に印刷要求を行うプリンタドライバプログラム、暗号化されたアプリケーションの文書を印刷するプリンタ装置に関する。

## 【0002】

## 【従来の技術】

たとえば、Adobe (R) 社の Acrobat Reader (R) のようなアプリケーションでは、文書内容を他人に閲覧できないようにするために、文書パスワードのような文書認証情報を入力して文書データを暗号化して保存する機能を備えている（非特許文献1 参照）。

## 【0003】

クライアント装置である PC (Personal Computer) でこのような暗号化された文書データを作成して、LAN (Local Area Network) などのネットワークに接続されたプリンタ装置で印刷する場合には、アプリケーション上で文書パスワードを入力して暗号化された文書を復号化してから、復号化された文書をプリンタドライバに渡し、プリンタドライバから復号化された文書ファイルをネットワーク上のプリンタ装置に送信してプリンタ装置でそのまま印刷している。

## 【0004】

また、このような暗号化された文書を他人が勝手に印刷することを回避するために、アプリケーションで文書を復号化して印刷要求を行う際に、プリンタドライバ側で印刷ジョブ毎のジョブパスワードをユーザに入力させる。そして、文書データを入力されたジョブパスワードとともにプリンタ装置に送信する。図17は、このような従来のプリンタドライバとプリンタ装置間を流れる印刷データの構造を示すデータ構造図である。図17に示すように、PJLジョブパスワード指定が印刷データであるPDF文書データ（平文）の先頭に付加されたデータ構造となっている。

## 【0005】

そして、プリンタ装置側ではユーザに認証パスワードを入力させて、正当な認証パスワードである場合にのみ印刷ジョブを開始して、文書を印刷するようになっている。

## 【0006】

## 【非特許文献1】

Adobe (R) 社ホームページ「Adobe AcrobatならPDFがもっと使える」 ([http://www.adobe.co.jp/acrofamily/features/acro\\_nikkei/page4.html](http://www.adobe.co.jp/acrofamily/features/acro_nikkei/page4.html))

#### 【0007】

##### 【発明が解決しようとする課題】

しかしながら、このような従来のプリンタドライバやプリンタ装置では、アプリケーション上で暗号化された文書であっても、印刷する段階で復号化しなければならないため、PCからプリンタ装置までのネットワーク上を平文の文書データが流れてしまい、悪意のある第三者によって平文の文書データが傍受されてしまうおそれがある。

#### 【0008】

また、印刷ジョブ毎のジョブパスワードによって悪意のある第三者による暗号化文書の印刷を防止してる場合であっても、ジョブパスワードが平文のために、ネットワーク上で第三者に傍受されてしまう可能性がある。また、プリンタ装置のハードディスク装置(HDD)やメモリなどの記憶媒体には復号化された文書データが一時的に保存されるため、プリンタ装置のシステム管理者が保存された平文の文書データを参照することができてしまう。

#### 【0009】

このように、従来のプリンタドライバやプリンタ装置では、アプリケーションで暗号化された文書データを印刷する場合に、セキュリティが低下してしまうという問題があった。

#### 【0010】

この発明は上記に鑑みてなされたもので、アプリケーションで暗号化された文書データを印刷する場合においてもセキュリティを向上させることができるプリンタドライバプログラムおよびプリンタ装置を得ることを目的とする。

#### 【0011】

##### 【課題を解決するための手段】

上記目的を達成するため、請求項1にかかる発明は、ネットワークに接続され

たプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラムであって、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、前記暗号化されたアプリ文書データと前記文書認証情報処理手順によって入力された文書認証情報とを含む印刷データを生成する印刷データ生成手順と、前記印刷データ生成手段によって生成された印刷データをネットワークに接続されたプリンタ装置に送信する送信手順と、をコンピュータに実行させるプリンタドライバプログラムである。

#### 【0 0 1 2】

この請求項 1 の発明によれば、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させ、暗号化されたアプリ文書データと入力された文書認証情報とを含む印刷データを生成してネットワークに接続されたプリンタ装置に送信することで、暗号化されたアプリ文書データを復号化せずにプリンタ装置に送信して、同時に送信する文書認証情報によってプリンタ装置側で復号化して印刷を行えるので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを防止することができる。また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データを暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができる。暗号化文書の印刷におけるセキュリティの向上を図ることができる。

#### 【0 0 1 3】

また、請求項 2 にかかる発明は、ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラムであって、前記プリンタ装置との間で予め定められた第 1 の鍵情報を前記プリンタ装置から取得して、第 1 の鍵情報に基づいて第 2 の鍵情報を生成する鍵生成手順と、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、前記文書認証情報処理手段によって入力された前記文書認証情報と前記暗号化されたアプリ文書データとを含む印刷データを生成する印刷データ生成手順と、前記鍵生成手段に

よって生成された第 2 の鍵情報によって前記印刷データを暗号化する暗号化手順と、前記暗号化手段によって暗号化された印刷データと前記第 2 の鍵情報を、ネットワークに接続されたプリンタ装置に送信する送信手順と、をコンピュータに実行させるプリンタドライバプログラムである。

#### 【 0 0 1 4 】

この請求項 2 の発明によれば、プリンタ装置から取得した第 1 の鍵情報から第 2 の鍵情報を生成し、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させ、入力された文書認証情報と暗号化されたアプリ文書データとを含む印刷データを生成し、生成された第 2 の鍵情報によって印刷データを暗号化し、暗号化された印刷データと第 2 の鍵情報をネットワークに接続されたプリンタ装置に送信することで、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を第 2 の鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができる。また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

#### 【 0 0 1 5 】

また、請求項 3 にかかる発明は、請求項 2 に記載のプリンタドライバプログラムにおいて、前記第 1 の鍵情報を前記プリンタ装置に要求する要求手順をさらにコンピュータに実行させるものである。

#### 【 0 0 1 6 】

この請求項 3 の発明によれば、第 1 の鍵情報を前記プリンタ装置に要求することで、印刷ジョブごとに異なる第 1 の鍵情報を取得することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

#### 【 0 0 1 7 】

また、請求項 4 にかかる発明は、請求項 2 に記載のプリンタドライバプログラ



ムにおいて、ネットワークに接続された時点で、接続通知を前記プリンタ装置に送信し、前記接続通知の送信後に、前記プリンタ装置から前記第1の鍵情報を受信する受信手順をさらにコンピュータに実行させるものである。

#### 【0018】

この請求項4の発明によれば、ネットワークに接続された時点で、接続通知をプリンタ装置に送信して、かかる接続通知の送信後にプリンタ装置から第1の鍵情報を受信することで、印刷する度に第1の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができる。

#### 【0019】

また、請求項5にかかる発明は、ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラムであって、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、前記文書認証情報処理手順によって入力された前記文書認証情報と前記暗号化されたアプリ文書データとを含む印刷データを生成する印刷データ生成手順と、プリンタ装置から取得した公開鍵情報によって前記印刷データを暗号化する暗号化手順と、前記暗号化手順によって暗号化された印刷データとクライアント装置に固有の識別情報を、ネットワークに接続されたプリンタ装置に送信する送信手順と、をコンピュータに実行させるプリンタドライバプログラムである。

#### 【0020】

この請求項5の発明によれば、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させ、入力された文書認証情報と暗号化されたアプリ文書データとを含む印刷データを生成し、プリンタ装置から取得した公開鍵情報によって印刷データを暗号化し、暗号化された印刷データとクライアント装置に固有の識別情報を、ネットワークに接続されたプリンタ装置に送信することで、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を公開鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある

第三者が傍受することを確実に防止することができる。また、プリンタ装置で秘密鍵情報を用いて復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

#### 【 0 0 2 1 】

また、請求項 6 にかかる発明は、請求項 5 に記載のプリンタドライバプログラムにおいて、前記公開鍵情報を前記プリンタ装置に要求する要求手順をさらにコンピュータに実行させるものである。

#### 【 0 0 2 2 】

この請求項 6 の発明によれば、公開鍵情報をプリンタ装置に要求することで、印刷ジョブごとに異なる公開鍵情報を取得することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

#### 【 0 0 2 3 】

また、請求項 7 にかかる発明は、請求項 5 に記載のプリンタドライバプログラムにおいて、ネットワークに接続された時点で、接続通知を前記プリンタ装置に送信し、前記接続通知を送信後に、前記プリンタ装置から前記公開鍵情報を受信する受信手順をさらにコンピュータに実行させるものである。

#### 【 0 0 2 4 】

この請求項 7 の発明によれば、ネットワークに接続された時点で、接続通知をプリンタ装置に送信し、かかる接続通知を送信後にプリンタ装置から公開鍵情報を受信することで、印刷する度に第 1 の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができる。

#### 【 0 0 2 5 】

また、請求項 8 にかかる発明は、請求項 2 ～ 7 のいずれか一つに記載のプリンタドライバプログラムにおいて、印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させるジョブ認証情報処理手順をさらにコンピュータに実行させ、前記印刷データ生成手順は、さらに前記ジョブ認証情報処理手順によって入力



された前記ジョブ認証情報を含む前記印刷データを生成することを特徴とする。

【 0 0 2 6 】

この請求項 8 の発明によれば、印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させ、入力されたジョブ認証情報を含む印刷データを生成することで、暗号化されたアプリ文書データの印刷時において、アプリ文書データを暗号化された状態のまま、さらに印刷ジョブ毎に認証を行うことができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

【 0 0 2 7 】

また、請求項 9 にかかる発明は、請求項 2 ～ 7 のいずれか一つに記載のプリンタドライバプログラムにおいて、前記文書認証情報処理手段によって入力された文書認証情報から印刷ジョブを開始させるためのジョブ認証情報を生成するジョブ認証情報処理手順をさらにコンピュータに実行させ、前記印刷データ生成手順は、さらに前記ジョブ認証情報処理手順によって生成された前記ジョブ認証情報を含む前記印刷データを生成することを特徴とするものである。

【 0 0 2 8 】

この請求項 9 の発明によれば、入力された文書認証情報から印刷ジョブを開始させるためのジョブ認証情報を生成し、ジョブ認証情報を含む印刷データを生成することで、印刷ジョブ毎に認証に必要なジョブ認証情報を、アプリ文書データの暗号化に必要な文書認証情報から自動的に生成することができるので、ユーザに何度も認証情報を入力させる手間が省け、ユーザの便宜となる。

【 0 0 2 9 】

また、請求項 1 0 にかかる発明は、請求項 9 に記載のプリンタドライバプログラムにおいて、前記ジョブ認証情報処理手順は、前記文書認証情報処理手段によって入力された文書認証情報と同一データを前記ジョブ認証情報として生成することを特徴とする。

【 0 0 3 0 】

この請求項 1 0 の発明によれば、入力された文書認証情報と同一データを前記

ジョブ認証情報として生成することで、文書認証情報からジョブ認証情報を簡易に生成することができ、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させつつ迅速に行うことができる。

#### 【 0 0 3 1 】

また、請求項 1 1 にかかる発明は、ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、前記クライアント装置から受信した印刷データに含まれる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、を備えたことを特徴とする。

#### 【 0 0 3 2 】

この請求項 1 1 の発明によれば、クライアント装置から受信した印刷データに含まれる文書認証情報によって暗号化されたアプリ文書データを復号化し、復号化されたアプリ文書データを印刷することで、アプリ文書データを暗号化されたままクライアント装置から受信して、同時に送信する文書認証情報によってプリンタ装置側で復号化して印刷を行えるので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを防止することができる。また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データを暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

#### 【 0 0 3 3 】

また、請求項 1 2 にかかる発明は、ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、前記クライアント装置との間で予め定められた第 1 の鍵情報を生成し、生成された前記第 1 の鍵情報を前記クライアント装置に送信する第 1 の鍵情報生成手段と、前記クライアント装置から受信した前記第 1 の鍵情報に関連する第 2 の鍵情報から前記第 1 の鍵情報を生成するとともに、前記クライアント装置から受信した印刷データを、前記第 1 の鍵情報によって復号化する復号化手段と、前記印刷データに含ま

れる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、を備えたことを特徴とする。

#### 【0034】

この請求項12の発明によれば、クライアント装置との間で予め定められた第1の鍵情報を生成し、生成された第1の鍵情報をクライアント装置に送信し、クライアント装置から受信した第2の鍵情報から第1の鍵情報を生成するとともに、クライアント装置から受信した印刷データを、第1の鍵情報によって復号化し、印刷データに含まれる文書認証情報によって暗号化されたアプリ文書データを復号化し、復号化されたアプリ文書データを印刷することで、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を第2の鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができる。また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

#### 【0035】

また、請求項13にかかる発明は、請求項12に記載のプリンタ装置において、前記第1の鍵生成手段は、前記クライアント装置から前記第1の鍵情報の要求を受信した場合に、前記第1の鍵情報を生成し、生成された前記第1の鍵情報を、直ちに要求のあった前記クライアント装置に送信することを特徴とする。

#### 【0036】

この請求項13の発明によれば、クライアント装置から前記第1の鍵情報の要求を受信した場合に、前記第1の鍵情報を生成し、生成された前記第1の鍵情報を、直ちに要求のあった前記クライアント装置に送信することで、要求された時点で直ちに印刷ジョブごとに異なる第1の鍵情報を送信することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

#### 【0037】

また、請求項 1 4 にかかる発明は、請求項 1 2 に記載のプリンタ装置において、前記第 1 の鍵生成手段は、前記クライアント装置から前記第 1 の鍵情報の要求を受信した場合に、前記第 1 の鍵情報を生成し、生成された前記第 1 の鍵情報を、印刷可能な状態となった時点で要求のあった前記クライアント装置に送信することを特徴とする。

#### 【 0 0 3 8 】

この請求項 1 4 の発明によれば、クライアント装置から第 1 の鍵情報の要求を受信した場合に、第 1 の鍵情報を生成し、生成された第 1 の鍵情報を、印刷可能な状態となった時点で要求のあった前記クライアント装置に送信することで、要求があった時点から印刷開始時までに時間差がある場合に、実際に印刷開始時に第 1 の鍵情報を送信することができるので、要求時点から印刷開始時点までの間に第三者が傍受することを回避することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

#### 【 0 0 3 9 】

また、請求項 1 5 にかかる発明は、請求項 1 2 に記載のプリンタ装置において、前記第 1 の鍵生成手段は、前記第 1 の鍵情報を生成し、前記クライアント装置がネットワークに接続された時点で前記クライアント装置に送信することを特徴とする。

#### 【 0 0 4 0 】

この請求項 1 5 の発明によれば、第 1 の鍵情報を生成し、クライアント装置がネットワークに接続された時点でクライアント装置に送信することで、クライアント装置側で印刷する度に第 1 の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができる。

#### 【 0 0 4 1 】

また、請求項 1 6 にかかる発明は、請求項 1 2 ～ 1 5 のいずれか一つに記載のプリンタ装置において、前記復号化手段は、前記クライアント装置から前記第 2 の鍵情報を受信した場合に、前記第 1 の鍵情報生成手段によって生成された前記第 1 の鍵情報と、受信した第 2 の鍵情報から生成された第 1 の鍵情報とを比較し

、両第 1 の鍵情報が一致する場合にのみ前記印刷データの復号化を行うことを特徴とする。

#### 【 0 0 4 2 】

この請求項 1 6 の発明によれば、クライアント装置から第 2 の鍵情報を受信した場合に、生成された第 1 の鍵情報と、受信した第 2 の鍵情報から生成された第 1 の鍵情報とを比較し、両第 1 の鍵情報が一致する場合にのみ印刷データの復号化を行うことで、第 1 の鍵情報の改ざんされた場合に暗号化されたアプリ文書データの印刷を未然に防止することができ、セキュリティの向上を図ることができる。

#### 【 0 0 4 3 】

また、請求項 1 7 にかかる発明は、ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、クライアント装置に固有の識別情報に対する秘密鍵情報から公開鍵情報を生成し、クライアント装置に送信する公開鍵処理手段と、前記クライアント装置から受信した印刷データを、前記クライアント装置から受信した識別情報に対応する秘密鍵情報によって復号化する復号化手段と、前記印刷データに含まれる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、を備えたことを特徴とする。

#### 【 0 0 4 4 】

この請求項 1 7 の発明によれば、クライアント装置に固有の識別情報に対する秘密鍵情報から公開鍵情報を生成し、クライアント装置に送信し、クライアント装置から受信した印刷データをクライアント装置から受信した識別情報に対応する秘密鍵情報によって復号化し、印刷データに含まれる文書認証情報によって暗号化されたアプリ文書データを復号化し、復号化されたアプリ文書データを印刷することで、アプリ文書データを暗号化された状態のまま、しかも復号化するための文書認証情報を公開鍵情報で暗号化された状態でクライアント装置から受信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができる。また、プリンタ装置で秘密鍵情報を用



いて復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

#### 【 0 0 4 5 】

また、請求項 1 8 にかかる発明は、請求項 1 7 に記載のプリンタ装置において、前記クライアント装置から前記公開鍵情報の要求を受信した場合に、前記秘密鍵情報を生成する秘密鍵生成手段と、前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を直ちに前記クライアント装置に送信する公開鍵処理手段と、をさらに備えたことを特徴とする。

#### 【 0 0 4 6 】

この請求項 1 8 の発明によれば、クライアント装置から公開鍵情報の要求を受信した場合に、秘密鍵情報を生成し、生成された秘密鍵情報から公開鍵情報を生成し、生成された公開鍵情報を直ちにクライアント装置に送信することで、要求された時点で直ちに印刷ジョブごとに異なる公開鍵情報を送信することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

#### 【 0 0 4 7 】

また、請求項 1 9 にかかる発明は、請求項 1 7 に記載のプリンタ装置において、前記クライアント装置から前記公開鍵情報の要求を受信した場合に、前記秘密鍵情報を生成する秘密鍵生成手段と、前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を、印刷可能な状態になった時点で前記クライアント装置に送信する公開鍵処理手段と、をさらに備えたことを特徴とする。

#### 【 0 0 4 8 】

この請求項 1 9 の発明によれば、クライアント装置から公開鍵情報の要求を受信した場合に秘密鍵情報を生成し、生成された秘密鍵情報から公開鍵情報を生成し、生成された前記公開鍵情報を、印刷可能な状態になった時点で前記クライアント装置に送信することで、要求があった時点から印刷開始時までに時間差がある場

合に、実際に印刷開始時に公開鍵情報を送信することができるので、要求時点から印刷開始時点までの間に第三者が傍受することを回避することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

#### 【 0 0 4 9 】

また、請求項 2 0 にかかる発明は、請求項 1 7 に記載のプリンタ装置において、前記クライアント装置に対する前記秘密鍵情報を生成する秘密鍵生成手段と、前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を、前記クライアント装置がネットワークに接続された時点で前記クライアント装置に送信する公開鍵処理手段と、をさらに備えたことを特徴とする。

#### 【 0 0 5 0 】

この請求項 2 0 の発明によれば、クライアント装置に対する秘密鍵情報を生成し、生成された秘密鍵情報から公開鍵情報を生成し、生成された公開鍵情報を、クライアント装置がネットワークに接続された時点でクライアント装置に送信することで、クライアント装置側で印刷する度に公開鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができる。

#### 【 0 0 5 1 】

また、請求項 2 1 にかかる発明は、請求項 1 7 ～ 2 0 のいずれか一つに記載のプリンタ装置において、前記クライアント装置の識別情報と前記秘密鍵情報と前記秘密鍵情報の有効期間とを対応付けた鍵管理情報を記憶する記憶手段をさらに備え、前記復号化手段は、前記クライアント装置から前記クライアント情報を受信した場合に、前記鍵管理情報を参照して、前記クライアント情報に対応する前記秘密鍵情報が前記有効期限の範囲内にあるか否かを判断し、前記有効期限の範囲内にある場合にのみ前記印刷データを復号化することを特徴とする。

#### 【 0 0 5 2 】

この請求項 2 1 の発明によれば、クライアント装置の識別情報と秘密鍵情報と秘密鍵情報の有効期間とを対応付けた鍵管理情報を記憶し、クライアント装置からクライアント情報を受信した場合に、鍵管理情報を参照してクライアント情報



に対応する秘密鍵情報が前記有効期限の範囲内にあるか否かを判断し、有効期限の範囲内にある場合にのみ印刷データを復号化することで、有効期限切れで第三の傍受されたおそれのある秘密鍵情報によるアプリ文書データの復号化および印刷を防止することができ、セキュリティをより向上させることができる。

#### 【 0 0 5 3 】

また、請求項 2 2 にかかる発明は、請求項 1 2 ～ 2 0 のいずれか一つに記載のプリンタ装置において、前記復号化手段は、印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させ、前記印刷データを復号化することを特徴とする。

#### 【 0 0 5 4 】

この請求項 2 2 の発明によれば、印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させ、前記印刷データを復号化することで、暗号化されたアプリ文書データの印刷時において、アプリ文書データを暗号化された状態のまま、さらに印刷ジョブ毎に認証を行うことができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

#### 【 0 0 5 5 】

##### 【発明の実施の形態】

以下に添付図面を参照して、この発明にかかるプリンタドライバプログラムおよびプリンタ装置の好適な実施の形態を詳細に説明する。

#### 【 0 0 5 6 】

##### （実施の形態 1）

図 1 は、この発明の実施の形態 1 であるクライアント装置（P C） 1 0 0 およびプリンタ装置 1 3 0 の機能的構成を示すブロック図である。この実施の形態 1 にかかる P C 1 0 0 では、P C 上のアプリケーション 1 2 0 である A c r o b a t （R）によって P D F 文書データを作成して暗号化し、文書パスワードの入力で復号化できる暗号化 P D F 文書データをそのまま（復号化せず）、プリンタ装置 1 3 0 に送信し、プリンタ装置 1 3 0 で印刷するようになっている。

#### 【 0 0 5 7 】

プリンタ装置 130 と PC 100 とは、LAN 151 等のネットワークによって接続されている。PC 100 は、図 1 に示すように、プリンタドライバ 110 がインストールされており、このプリンタドライバ 110 は、PDL 処理部 111 と、文書パスワード処理部 112 と、ユーザインタフェース部 113 と、ホスト I/F 制御部 114 とを主に備えている。

#### 【0058】

文書パスワード処理部 112 は、アプリケーション 120 内部で暗号化された PDF 文書データを復号化するために必要な文書パスワードの入力指示を要求し、入力された文書パスワードを受け付ける。そして、ユーザから入力された文書パスワードを PJL 文書パスワード指定データとして暗号化 PDF 文書データの先頭に付加する。そして、PJL 文書パスワード指定データが付加された暗号化 PDF 文書データの後尾に印刷ジョブに関するデータである PJL データを付加する。そして、これらの PJL 文書パスワード指定データと PJL データとが付加された暗号化 PDF 文書データとを印刷データとする。この文書パスワードは、本発明における文書認証情報を構成する。

#### 【0059】

PDL 処理部 111 は、PDF 文書データ（暗号化されていないデータ）の印刷の際に使用されるものであり、暗号化されていない PDF 文書データの印刷文書データを PDL データ（PDL：Page Description Language：ページ記述言語）に変換して印刷データを生成するものである。

#### 【0060】

ユーザインタフェース部 113 は、モニタ 115 に各種画面を表示するとともに、ユーザによるキーボード 116 からの入力イベントを受け付けるものである。

#### 【0061】

ホスト I/F 制御部 114 は、暗号化された PDF 文書データをホスト I/F 117 から LAN 151 を介してプリンタ装置 130 に送信するものである。

#### 【0062】

プリンタ装置 130 には、プリンタコントローラ 140 が装着されており、こ

のプリンタコントローラ 140 は、PDL 処理部 142 と、PJL 処理部 141 と、ホスト I/F 制御部 143 と、パネル制御部 144 と、蓄積制御部 145 と、印刷制御部 146 とを主に備えている。

#### 【0063】

PJL 処理部 141 は、PC100 から受信した印刷データの先頭に付加されたプリンタジョブ言語 (PJL: Printer Job Language) で記述された PJL 文書パスワード指定を解釈して、文書パスワードを取得するものである。PJL 処理部 141 は、この他刷ジョブに関する各種制御を行う。

#### 【0064】

PDL 処理部 142 は、PJL 処理部 141 によって取得された文書パスワードの正当性を判断し、正当である場合には、この文書パスワードを用いて暗号化された PDF 文書データを復号化し、描画データを生成する。この PDL 処理部 142 は、本発明における文書復号化手段を構成する。

#### 【0065】

ホスト I/F 制御部 143 は、LAN115、ホスト I/F 147 を介して PC100 から印刷データを受信するものである。

#### 【0066】

パネル制御部 144 は、操作パネル 148 に対する表示出力、入力イベントの取得などを制御するものである。蓄積制御部 145 は、ハードディスク装置 (HDD) 149 やメモリに対するリード/ライトを制御するものである。印刷制御部 146 は、印刷エンジン 150 に対する印刷要求を制御するものである。

#### 【0067】

次に、以上のように構成された本実施の形態のプリンタドライバおよびプリンタ装置 130 による暗号化 PDF 文書データの印刷処理について説明する。図 2 は、本実施の形態のプリンタドライバおよびプリンタ装置 130 による暗号化 PDF 文書データの印刷処理の手順を示すフローチャートである。

#### 【0068】

まず、ユーザがアプリケーション 120 (Acrobat (R) または Acrobat Reader (R)) で PDF 文書を文書パスワードによって暗号化

し、暗号化した状態のままアプリケーション 1 2 0 の印刷画面でプリンタ装置 1 3 0 の I P アドレスを指定して印刷コマンドを発行した場合を考える。

#### 【 0 0 6 9 】

このとき、プリンタドライバ 1 1 0 では、文書パスワード処理部 1 1 2 が文書パスワード入力画面の表示要求をユーザインタフェース部 1 1 3 に対して行うことにより、ユーザインタフェース部 1 1 3 は文書パスワード入力画面をモニタ 1 1 5 に表示する（ステップ S 2 0 1）。

#### 【 0 0 7 0 】

ユーザが文書パスワード入力画面から暗号化 P D F 文書データに対する文書パスワードをキーボード 1 1 6 から入力すると、そのキーイベントをユーザインタフェース部 1 1 3 が取得する。そして、文書パスワード処理部 1 1 2 は、取得した文書パスワードを P J L 文書パスワード指定データとして暗号化 P D F 文書データの先頭に付加する（ステップ S 2 0 2）。そして、文書パスワード処理部 1 1 2 によって、P J L 文書パスワード指定データが付加された暗号化 P D F 文書データの後尾に P J L データを付加し、これらのデータを印刷データとして生成する（ステップ S 2 0 3）。生成された印刷データは、ホスト I / F 制御部 1 1 4 によって、プリンタ装置 1 3 0 に送信される（ステップ S 2 0 4）。

#### 【 0 0 7 1 】

図 4 は、本実施の形態のプリンタドライバ 1 1 0 で生成される印刷データの構造を示すデータ構造図である。図 2 に示すように、印刷データは、P J L 文書パスワード指定（平文）と暗号化 P D F 文書データと P J L データとから構成される。なお、P J L データは付加されていない場合もある。

#### 【 0 0 7 2 】

プリンタ装置 1 3 0 では、ホスト I / F 制御部 1 4 3 で印刷データを受信して（ステップ S 2 0 5）、受信した印刷データのデータ解釈処理を行い（ステップ S 2 0 6）、印刷制御部 1 4 6 によって印刷実行を行う（ステップ S 2 0 7）。

#### 【 0 0 7 3 】

ここで、印刷データの解釈処理について説明する。図 3 は、印刷データの解釈処理の手順を示すフローチャートである。まず、P J L 処理部 1 4 1 によって、

印刷データに含まれる P J L 文書パスワード指定を解釈し、文書パスワードを取得する（ステップ S 3 0 1）。そして、P D L 処理部 1 4 2 によって、取得した文書パスワードと暗号化 P D F 文書データに含まれる文書パスワードとが一致するか否かをチェックすることにより、印刷データに含まれた文書パスワードの正当性を判断する（ステップ S 3 0 2）。ここで、暗号化 P D F 文書データに含まれる文書パスワードの取得は、アプリケーション 1 2 0 に提供されるパスワード取得関数を呼び出すことにより行う。

#### 【 0 0 7 4 】

そして、両文書パスワードが一致する場合には、文書パスワードが正当であると判断し、P D L 処理部 1 4 2 によって暗号化 P D F 文書データを復号化して、描画データを生成する（ステップ S 3 0 3）。一方、両文書パスワードが一致しない場合には、文書パスワードが不当であると判断し、印刷データを破棄して印刷処理の実行は行わない（ステップ S 3 0 4）。

#### 【 0 0 7 5 】

このように実施の形態 1 のプリンタドライバ 1 1 0 およびプリンタ装置 1 3 0 では、アプリケーション 1 2 0 によって暗号化されたアプリ文書データを復号化するための文書パスワードと、暗号化された P D F 文書データを含む印刷データをネットワークに接続されたプリンタ装置 1 3 0 に送信しているので、暗号化された P D F 文書データを復号化せずにプリンタ装置 1 3 0 に送信して、同時に送信する文書パスワードによってプリンタ装置 1 3 0 側で復号化して印刷を行えるので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを防止することができる。また、プリンタ装置 1 3 0 で復号化するまで H D D 1 4 9 などに P D F 文書データを暗号化された状態で保存することができるので、悪意のあるシステム管理者によって P D F 文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

#### 【 0 0 7 6 】

（実施の形態 2）

図 5 は、実施の形態 2 のクライアント装置（P C） 5 0 0 およびプリンタ装置



530の機能的構成を示すブロック図である。この実施の形態2にかかるPC500では、PC上のアプリケーション120であるAcrobat(R)によってPDF文書データを作成して暗号化し、文書パスワードと文書パスワードの入力で復号化できる暗号化PDF文書データを、PC500とプリンタ装置530との間で定められたSEEDによって暗号化して、プリンタ装置130に送信し、プリンタ装置530でSEED元によって復号化して印刷するようになっている。

#### 【0077】

プリンタ装置530とPC500とは、LAN151等のネットワークによって接続されている。PC500は、図5に示すように、プリンタドライバ510がインストールされており、このプリンタドライバ110は、PDL処理部111と、文書パスワード処理部112と、SEED生成部511と、暗号化部512と、ジョブ制御部513と、ユーザインタフェース部113と、ホストI/F制御部114とを主に備えている。

#### 【0078】

文書パスワード処理部112は、アプリケーション120内部で暗号化されたPDF文書データを復号化するために必要な文書パスワードの入力指示を要求し、入力された文書パスワードを受け付ける。そして、ユーザから入力された文書パスワードをPJL文書パスワード指定データとして暗号化PDF文書データの先頭に付加する。その他の機能は実施の形態1と文書パスワード処理部と同様である。

#### 【0079】

ジョブ制御部513は、プリンタ装置530に対して、SEED元の要求を行うものであり、SEED生成部511は、プリンタ装置530から受信したSEED元からSEEDを生成するものである。

#### 【0080】

暗号化部512は、生成されたSEEDによって、PJL文書パスワード指定データ、暗号化PDF文書データ、および印刷ジョブに関するデータであるPJLデータを暗号化するものである。なお、PDL処理部111は、実施の形態1

と同様の機能を有する。

#### 【0081】

ユーザインタフェース部 1 1 3 は、実施の形態 1 のプリンタドライバ 1 1 0 と同様の機能を有する。ホスト I / F 制御部 1 1 4 は、印刷データと S E E D をホスト I / F 1 1 7 から L A N 1 5 1 を介してプリンタ装置 1 3 0 に送信するものである。

#### 【0082】

プリンタ装置 5 3 0 には、プリンタコントローラ 5 4 0 が装着されており、このプリンタコントローラ 5 4 0 は、復号化部 5 4 1 と、S E E D 元生成部 5 4 2 と、P D L 処理部 1 4 2 と、P J L 処理部 1 4 1 と、ホスト I / F 制御部 1 4 3 と、パネル制御部 1 4 4 と、蓄積制御部 1 4 5 と、印刷制御部 1 4 6 とを主に備えている。

#### 【0083】

S E E D 元生成部 5 4 2 は、要求を行った P C 5 0 0 に対して S E E D 元を生成して送信するものである。

#### 【0084】

復号化部 5 4 1 は、P C 5 0 0 から送信されてきた S E E D の正当性の判断を行い、正当である場合に P C 5 0 0 から送信されてきた印刷データを S E E D によって復号化するものである。

#### 【0085】

P J L 処理部 1 4 1 は、P C 5 0 0 から受信した印刷データに付加されたプリンタジョブ言語 ( P J L : P r i n t e r J o b L a n g u a g e ) で記述された P J L 文書パスワード指定を解釈して、文書パスワードを取得するものである。P J L 処理部 1 4 1 は、この他刷ジョブに関する各種制御を行う。

#### 【0086】

P D L 処理部 1 4 2 は、P J L 処理部 1 4 1 によって取得された文書パスワードの正当性を判断し、正当である場合には、この文書パスワードを用いて暗号化された P D F 文書データを復号化し、描画データを生成する。この P D L 処理部 1 4 2 は、本発明における文書復号化手段を構成する。



**【0087】**

ホスト I/F 制御部、パネル制御部 144、蓄積制御部 145 および印刷制御部 146 は、実施の形態 1 のプリンタコントローラ 140 と同様の機能を有する。

**【0088】**

次に、以上のように構成された本実施の形態のプリンタドライバ 510 およびプリンタ装置 530 による暗号化 PDF 文書データの印刷処理について説明する。図 6 は、本実施の形態のプリンタドライバ 510 およびプリンタ装置 530 による暗号化 PDF 文書データの印刷処理の手順を示すフローチャートである。

**【0089】**

まず、ユーザがアプリケーション 120 (Acrobat (R) または Acrobat Reader (R)) で PDF 文書を文書パスワードによって暗号化し、暗号化した状態のままアプリケーション 120 の印刷画面でプリンタ装置 130 の IP アドレスを指定して印刷コマンドを発行した場合を考える。

**【0090】**

このとき、ジョブ制御部 513 によって、PC 500 のクライアント情報である IP アドレスと、印刷通知と、SEED 元要求とをプリンタ装置 530 に送信する (ステップ S601)。

**【0091】**

IP アドレスと、印刷通知と、SEED 元要求とを受信したプリンタ装置 530 では、SEED 元生成部 542 によって IP アドレスに固有の SEED を生成し、要求元の PC 500 に送信する (ステップ S602)。ここで、SEED を生成および送信するタイミングとしては、要求を受けて直ちに行う他、要求を受けてプリンタ装置 530 が印刷可能となった時点で送信するように構成することができる。

**【0092】**

PC 500 では、ホスト I/F 制御部 114 で SEED 元を受信すると (ステップ S603)、SEED 生成部 511 によって受信した SEED 元から SEED を生成する (ステップ S604)。

## 【0093】

そして、文書パスワード処理部112が文書パスワード入力画面の表示要求をユーザインタフェース部113に対して行うことにより、ユーザインタフェース部113は文書パスワード入力画面をモニタ115に表示する（ステップS605）。

## 【0094】

ユーザが文書パスワード入力画面から暗号化PDF文書データに対する文書パスワードをキーボード116から入力すると、そのキーイベントをユーザインタフェース部113が取得する。そして、文書パスワード処理部112は、取得した文書パスワードをPJL文書パスワード指定データとして暗号化PDF文書データの先頭に付加する（ステップS606）。そして、文書パスワード処理部112によって、PJL文書パスワード指定データが付加された暗号化PDF文書データの後尾にPJLデータを付加し、暗号化部512によってこれら3つのデータをSEEDによって暗号化する（ステップS607）。

## 【0095】

次に、PJL文書パスワード指定、暗号化PDF文書データおよびPJLデータの3つのデータを暗号化したデータを印刷データとして生成する（ステップS608）。生成された印刷データは、SEEDとともに、ホストI/F制御部114によってプリンタ装置130に送信される（ステップS609）。

## 【0096】

図7は、本実施の形態のプリンタドライバ510で生成される印刷データの構造を示すデータ構造図である。図7に示すように、印刷データは、先頭にSEEDが付加されており、PJL文書パスワード指定（暗号化）と暗号化PDF文書データ（暗号化）とPJLデータ（暗号化）とから構成される。なお、PJLデータは付加されていない場合もある。

## 【0097】

プリンタ装置130では、ホストI/F制御部143で印刷データを受信して（ステップS610）、復号化部541によって受信したSEEDをSEED元に復号化する（ステップS611）。復号化部541によって、復号化したSE

ED元と、SEED元生成部542によってステップS602で生成したSEED元とが一致するか否かを調べることにより、SEED元の正当性を判断する（ステップS612）。そして、一致する場合には受信したSEEDが正当であると判断し、復号化部542によってSEED元により印刷データを復号化する（ステップS613）。一方、両SEED元が一致しない場合には、受信したSEEDが不当なものである、すなわちSEEDが改ざん等されていると判断し、受信した印刷データを破棄し復号化処理を行わない（ステップS614）。

#### 【0098】

そして、復号化された印刷データのデータ解釈処理を行い（ステップS615）、印刷制御部146によって印刷実行を行う（ステップS616）。ここで、データ解釈処理については実施の形態1のプリンタコントローラ140と同様の処理で行われる。

#### 【0099】

なお、本実施の形態では、暗号化PDF文書データの印刷時にプリンタドライバ510からSEED元の要求をプリンタ装置530に行って、SEED元を取得しているが、この他、プリンタ装置530のホストI/F制御部143によってネットワーク上でPC500が接続されたことのブロードキャストメッセージをPC500から受信して接続を検知した場合に、SEED元を生成して新たに接続されたPC500に送信するように構成してもよい。この場合、PC500がネットワークに接続された場合、プリンタドライバ510のホストI/F制御部114によって接続通知のブロードキャストメッセージをプリンタ装置530に送信するように構成すれば良い。

#### 【0100】

このように実施の形態2のプリンタドライバ510およびプリンタ装置530では、プリンタ装置530から取得しSEED元からSEEDを生成し、アプリケーション120によって暗号化されたPDF文書データを復号化するための文書パスワードと暗号化されたPDF文書データとを含む印刷データをSEEDによって暗号化し、暗号化された印刷データとSEEDをネットワークに接続されたプリンタ装置530に送信して、プリンタ装置530で復号化して印刷してい

る。すなわち、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書パスワードを S E E D で暗号化してプリンタ装置に送信するので、P D F 文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができる。また、プリンタ装置 5 3 0 で復号化するまで記憶媒体などに P D F 文書データと文書パスワードを暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

#### 【 0 1 0 1 】

なお、本実施の形態では、文書パスワードと暗号化 P D F 文書データの両方を S E E D で暗号化して印刷データを生成しているが、文書パスワードのみを S E E D で暗号化して暗号化 P D F 文書データはそのまま印刷データを生成してもよい。これは、P D F 文書データはすでに文書パスワードによって暗号化されているからである。

#### 【 0 1 0 2 】

(実施の形態 3)

図 8 は、実施の形態 3 のクライアント装置 ( P C ) 8 0 0 およびプリンタ装置 8 3 0 の機能的構成を示すブロック図である。この実施の形態 3 にかかる P C 8 0 0 では、P C 上のアプリケーション 1 2 0 である A c r o b a t ( R ) によって P D F 文書データを作成して暗号化し、文書パスワードと文書パスワードの入力で復号化できる暗号化 P D F 文書データを、公開鍵で暗号化して、プリンタ装置 8 3 0 に送信し、プリンタ装置 8 3 0 で秘密鍵で復号化して印刷するようになっている。

#### 【 0 1 0 3 】

プリンタ装置 8 3 0 と P C 8 0 0 とは、L A N 1 5 1 等のネットワークによって接続されている。P C 8 0 0 は、図 8 に示すように、プリンタドライバ 8 1 0 がインストールされており、このプリンタドライバ 8 1 0 は、P D L 処理部 1 1 1 と、文書パスワード処理部 1 1 2 と、暗号化部 8 1 2 と、ジョブ制御部 8 1 3 と、ユーザインタフェース部 1 1 3 と、ホスト I / F 制御部 1 1 4 とを主に備え

ている。

#### 【 0 1 0 4 】

文書パスワード処理部 1 1 2 は、アプリケーション 1 2 0 内部で暗号化された P D F 文書データを復号化するために必要な文書パスワードの入力指示を要求し、入力された文書パスワードを受け付ける。そして、ユーザから入力された文書パスワードを P J L 文書パスワード指定データとして暗号化 P D F 文書データの先頭に付加する。その他の機能は実施の形態 1 と同様である。

#### 【 0 1 0 5 】

ジョブ制御部 8 1 3 は、プリンタ装置 8 3 0 に対して、公開鍵の要求を行うものである。暗号化部 8 1 2 は、プリンタ装置 8 3 0 から受信した公開鍵によって、P J L 文書パスワード指定データ、暗号化 P D F 文書データ、および印刷ジョブに関するデータである P J L データを暗号化するものである。P D L 処理部 1 1 1 は、実施の形態 1 の P D L 処理部 1 1 1 と同様の機能を有する。

#### 【 0 1 0 6 】

ユーザインタフェース部 1 1 3 は、実施の形態 1 のプリンタドライバ 1 1 0 と同様の機能を有する。ホスト I / F 制御部 1 1 4 は、印刷データとクライアント情報（I P アドレス）をホスト I / F 1 1 7 から L A N 1 5 1 を介してプリンタ装置 1 3 0 に送信するものである。

#### 【 0 1 0 7 】

プリンタ装置 8 3 0 には、プリンタコントローラ 8 4 0 が装着されており、このプリンタコントローラ 8 4 0 は、復号化部 8 4 1 と、秘密鍵生成部と 8 4 2 と、公開鍵処理部 8 4 3 と、P D L 処理部 1 4 2 と、P J L 処理部 1 4 1 と、ホスト I / F 制御部 1 4 3 と、パネル制御部 1 4 4 と、蓄積制御部 1 4 5 と、印刷制御部 1 4 6 とを主に備えている。

#### 【 0 1 0 8 】

秘密鍵生成部 8 4 2 は、要求を行った P C 8 0 0 に対する秘密鍵を生成するものである。公開鍵処理部 8 4 3 は、秘密鍵から公開鍵を生成して鍵テーブルに登録し、また生成された公開鍵を要求元の P C 8 0 0 に送信するものである。

#### 【 0 1 0 9 】

復号化部 8 4 1 は、P C 8 0 0 から送信されてきた公開鍵の正当性の判断を行い、正当である場合に P C 8 0 0 から送信されてきた印刷データを公開鍵に対応する秘密鍵によって復号化するものである。

#### 【 0 1 1 0 】

P J L 処理部 1 4 1 は、P C 5 0 0 から受信した印刷データに付加されたプリンタジョブ言語 ( P J L : P r i n t e r J o b L a n g u a g e ) で記述された P J L 文書パスワード指定を解釈して、文書パスワードを取得するものである。P J L 処理部 1 4 1 は、この他刷ジョブに関する各種制御を行う。

#### 【 0 1 1 1 】

P D L 処理部 1 4 2 は、P J L 処理部 1 4 1 によって取得された文書パスワードの正当性を判断し、正当である場合には、この文書パスワードを用いて暗号化された P D F 文書データを復号化し、描画データを生成する。

#### 【 0 1 1 2 】

ホスト I / F 制御部、パネル制御部 1 4 4、蓄積制御部 1 4 5 および印刷制御部 1 4 6 は、実施の形態 1 のプリンタコントローラ 1 4 0 と同様の機能を有する。

#### 【 0 1 1 3 】

次に、以上のように構成された本実施の形態のプリンタドライバ 8 1 0 およびプリンタ装置 8 3 0 による暗号化 P D F 文書データの印刷処理について説明する。図 9 は、本実施の形態のプリンタドライバ 8 1 0 およびプリンタ装置 8 3 0 による暗号化 P D F 文書データの印刷処理の手順を示すフローチャートである。

#### 【 0 1 1 4 】

まず、ユーザがアプリケーション 1 2 0 ( A c r o b a t ( R ) または A c r o b a t R e a d e r ( R ) ) で P D F 文書を文書パスワードによって暗号化し、暗号化した状態のままアプリケーション 1 2 0 の印刷画面でプリンタ装置 1 3 0 の I P アドレスを指定して印刷コマンドを発行した場合を考える。

#### 【 0 1 1 5 】

このとき、ジョブ制御部 8 1 3 によって、P C 8 0 0 のクライアント情報である I P アドレスと、印刷通知と、公開鍵要求とをプリンタ装置 8 3 0 に送信する



(ステップ S 9 0 1)。

#### 【 0 1 1 6 】

I P アドレスと、印刷通知と、公開鍵要求とを受信したプリンタ装置 8 3 0 では、秘密鍵生成部 8 4 2 によって I P アドレスに固有の秘密鍵を生成する (ステップ S 9 0 2)。そして、公開鍵処理部 8 4 3 によって、この秘密鍵から公開鍵を生成し、要求元の P C 8 0 0 に送信する (ステップ S 9 0 3)。ここで、公開鍵の生成および送信するタイミングとしては、要求を受けて直ちに行う他、要求を受けてプリンタ装置 8 3 0 が印刷可能となった時点で送信するように構成することができる。公開鍵を生成すると、公開鍵処理部 8 4 3 によって、鍵テーブルを H D D 1 4 9 に生成し、生成された公開鍵、秘密鍵を登録する (ステップ S 9 0 4)。

#### 【 0 1 1 7 】

図 1 0 は、鍵テーブルのデータ構造図である。図 1 0 に示すように、鍵テーブルは、クライアント情報である I P アドレスと公開鍵と秘密鍵と鍵の有効期限とから構成される。

#### 【 0 1 1 8 】

P C 8 0 0 では、ホスト I / F 制御部 1 1 4 で公開鍵を受信すると (ステップ S 9 0 5)、文書パスワード処理部 1 1 2 が文書パスワード入力画面の表示要求をユーザインタフェース部 1 1 3 に対して行うことにより、ユーザインタフェース部 1 1 3 は文書パスワード入力画面をモニタ 1 1 5 に表示する (ステップ S 9 0 6)。

#### 【 0 1 1 9 】

ユーザが文書パスワード入力画面から暗号化 P D F 文書データに対する文書パスワードをキーボード 1 1 6 から入力すると、そのキーイベントをユーザインタフェース部 1 1 3 が取得する。そして、文書パスワード処理部 1 1 2 は、取得した文書パスワードを P J L 文書パスワード指定データとして暗号化 P D F 文書データの先頭に付加する (ステップ S 9 0 7)。そして、P J L 文書パスワード指定データが付加された暗号化 P D F 文書データの後尾に P J L データを付加し、暗号化部 8 1 2 によってこれら 3 つのデータを公開鍵によって暗号化する (ステ



ップ S 9 0 8)。

#### 【 0 1 2 0 】

次に、P J L 文書パスワード指定、暗号化 P D F 文書データおよび P J L データの 3 つのデータを暗号化したデータを印刷データとして生成する (ステップ S 9 0 9)。生成された印刷データは、P C 8 0 0 のクライアント情報である I P アドレスとともに、ホスト I / F 制御部 1 1 4 によってプリンタ装置 8 3 0 に送信される (ステップ S 9 1 0)。

#### 【 0 1 2 1 】

図 1 1 は、本実施の形態のプリンタドライバ 8 1 0 で生成される印刷データの構造を示すデータ構造図である。図 1 1 に示すように、印刷データは、先頭にクライアント情報 (I P アドレス) が付加されており、P J L 文書パスワード指定 (暗号化) と暗号化 P D F 文書データ (暗号化) と P J L データ (暗号化) とから構成される。なお、P J L データは付加されていない場合もある。

#### 【 0 1 2 2 】

プリンタ装置 8 3 0 では、ホスト I / F 制御部 1 4 3 で印刷データを受信して (ステップ S 9 1 1)、復号化部 8 4 1 によって、鍵テーブルを参照し、受信した I P アドレスのクライアント情報に対応する公開鍵が有効であるか否かを判断する (ステップ S 9 1 2)。そして、有効である場合には、復号化部 5 4 2 によって秘密鍵で印刷データを復号化する (ステップ S 9 1 3)。一方、公開鍵が有効でない場合には、受信した印刷データを破棄し復号化処理を行わない (ステップ S 9 1 6)。

#### 【 0 1 2 3 】

そして、復号化された印刷データのデータ解釈処理を行い (ステップ S 9 1 4)、印刷制御部 1 4 6 によって印刷実行を行う (ステップ S 9 1 5)。ここで、データ解釈処理については実施の形態 1 のプリンタコントローラ 1 4 0 と同様の処理で行われる。

#### 【 0 1 2 4 】

なお、本実施の形態では、暗号化 P D F 文書データの印刷時にプリンタドライバ 8 1 0 から公開鍵の要求をプリンタ装置 8 3 0 に行って公開鍵を取得している

が、この他、プリンタ装置 8 3 0 のホスト I / F 制御部 1 4 3 によってネットワーク上で P C 8 0 0 が接続されたことのブロードキャストメッセージを P C 8 0 0 から受信して接続を検知した場合に、秘密鍵、公開鍵を生成して新たに接続された P C 8 0 0 に送信するように構成してもよい。この場合、P C 5 0 0 がネットワークに接続された場合、プリンタドライバ 8 1 0 のホスト I / F 制御部 1 1 4 によって接続通知のブロードキャストメッセージをプリンタ装置 8 3 0 に送信するように構成すれば良い。

#### 【 0 1 2 5 】

このように実施の形態 3 のプリンタドライバ 8 1 0 およびプリンタ装置 8 3 0 では、暗号化された P D F 文書データを復号化せずに、しかも復号化するための文書パスワードを公開鍵で暗号化してプリンタ装置 8 3 0 に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができる。また、プリンタ装置 8 3 0 で秘密鍵を用いて復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

#### 【 0 1 2 6 】

なお、本実施の形態では、文書パスワードと暗号化 P D F 文書データの両方を公開鍵で暗号化して印刷データを生成しているが、文書パスワードのみを公開鍵で暗号化して暗号化 P D F 文書データはそのまま印刷データを生成してもよい。これは、P D F 文書データはすでに文書パスワードによって暗号化されているからである。

#### 【 0 1 2 7 】

(実施の形態 4)

図 1 2 は、実施の形態 4 のクライアント装置 ( P C ) 1 2 0 0 およびプリンタ装置 1 2 3 0 の機能的構成を示すブロック図である。この実施の形態 4 にかかる P C 1 2 0 0 では、P C 上のアプリケーション 1 2 0 である A c r o b a t ( R ) によって P D F 文書データを作成して暗号化し、文書パスワードと文書パスワ

ードの入力で復号化できる暗号化PDF文書データを公開鍵で暗号化してプリンタ送信すると共に、印刷ジョブに対するジョブパスワードをプリンタ装置830に送信し、プリンタ装置1230で秘密鍵で復号化して印刷するようになっている。

#### 【0128】

プリンタ装置1230とPC1200とは、LAN151等のネットワークによって接続されている。PC1200は、図12に示すように、プリンタドライバ1210がインストールされており、このプリンタドライバ1210は、PDL処理部1212と、文書パスワード処理部112と、ジョブパスワード処理部1211と、暗号化部812と、ジョブ制御部813と、ユーザインタフェース部113と、ホストI/F制御部114とを主に備えている。

#### 【0129】

ジョブパスワード処理部1211は、印刷ジョブに対するジョブパスワードの入力指示を要求し、入力されたジョブパスワードを受け付ける。そして、ユーザから入力されたジョブパスワードをPJLジョブパスワード指定データとして暗号化PDF文書データに付加する。このジョブパスワードは、本発明におけるジョブ認証情報を構成する。PDL処理部1212は、実施の形態1のPDL処理部111と同様の機能を有する。

#### 【0130】

文書パスワード処理部112、ユーザインタフェース部113、ホストI/F制御部114は、実施の形態3のプリンタドライバと同様の機能を有する。

#### 【0131】

プリンタ装置1230には、プリンタコントローラ1240が装着されており、このプリンタコントローラ1240は、復号化部1254と、秘密鍵生成部842と、公開鍵処理部843と、PDL処理部142と、PJL処理部141と、ホストI/F制御部143と、パネル制御部144と、蓄積制御部145と、印刷制御部146とを主に備えている。

#### 【0132】

PJL処理部141は、PC500から受信した印刷データに付加されたプリ

ンタジョブ言語（P J L : P r i n t e r J o b L a n g u a g e）で記述されたP J L文書パスワード指定を解釈して文書パスワードを取得するとともに、P J Lジョブパスワード指定を解釈してジョブパスワードを取得するものである。P J L処理部141は、この他刷ジョブに関する各種制御を行う。

#### 【0133】

復号化部841、秘密鍵生成部と842、公開鍵処理部843、P D L処理部142、ホストI/F制御部143、パネル制御部144、蓄積制御部145は、実施の形態3のプリンタ装置と同様の機能を有している。

#### 【0134】

次に、以上のように構成された本実施の形態のプリンタドライバ1210およびプリンタ装置1230による暗号化P D F文書データの印刷処理について説明する。図13は、本実施の形態のプリンタドライバ1210およびプリンタ装置1230による暗号化P D F文書データの印刷処理の手順を示すフローチャートである。

#### 【0135】

まず、ユーザがアプリケーション120（A c r o b a t（R）またはA c r o b a t R e a d e r（R））でP D F文書を文書パスワードによって暗号化し、暗号化した状態のままアプリケーション120の印刷画面でプリンタ装置1230のI Pアドレスを指定して印刷コマンドを発行した場合を考える。

#### 【0136】

このとき、ジョブ制御部813によって、P C 1200のクライアント情報であるI Pアドレスと、印刷通知と、公開鍵要求とをプリンタ装置1230に送信する（ステップS 1301）。

#### 【0137】

I Pアドレスと、印刷通知と、公開鍵要求とを受信したプリンタ装置1230では、秘密鍵生成部842によってI Pアドレスに固有の秘密鍵を生成する（ステップS 1302）。そして、公開鍵処理部843によって、この秘密鍵から公開鍵を生成し、要求元のP C 800に送信する（ステップS 1303）。ここで、公開鍵の生成および送信するタイミングとしては、要求を受けて直ちに行う他

、要求を受けてプリンタ装置 830 が印刷可能となった時点で送信するように構成することができる。公開鍵を生成すると、公開鍵処理部 843 によって、鍵テーブルを HDD 149 に生成し、生成された公開鍵、秘密鍵を登録する（ステップ S1304）。

#### 【0138】

PC1200 では、ホスト I/F 制御部 114 で公開鍵を受信すると（ステップ S1305）、文書パスワード処理部 112 が文書パスワード入力画面の表示要求を、ジョブパスワード処理部 1211 がジョブパスワード入力画面の表示要求をそれぞれユーザインタフェース部 113 に対して行うことにより、ユーザインタフェース部 113 は文書パスワードおよびジョブパスワード入力画面をモニタ 115 に表示する（ステップ S1306）。

#### 【0139】

ユーザが文書パスワード入力画面から暗号化 PDF 文書データに対する文書パスワードを、印刷ジョブに対するジョブパスワードをキーボード 116 からそれぞれ入力すると、そのキーイベントをユーザインタフェース部 113 が取得する。そして、文書パスワード処理部 112 は取得した文書パスワードを P J L 文書パスワード指定データとして暗号化 PDF 文書データに付加し、ジョブパスワード処理部 1211 は取得したジョブパスワードを P J L ジョブパスワード指定データとして暗号化 PDF 文書データに付加する（ステップ S1307）。

#### 【0140】

そして、P J L 文書パスワード指定データと P J L ジョブパスワード指定データが付加された暗号化 PDF 文書データの後尾に P J L データを付加し、暗号化部 812 によってこれら 3 つのデータを公開鍵によって暗号化する（ステップ S1308）。

#### 【0141】

次に、P J L 文書パスワード指定、P J L ジョブパスワード指定、暗号化 PDF 文書データおよび P J L データの 4 つのデータを暗号化したデータからページ記述言語を用いて印刷データを生成する（ステップ S1309）。生成された印刷データは、PC800 のクライアント情報である IP アドレスとともに、ホス



ト I / F 制御部 1 1 4 によってプリンタ装置 8 3 0 に送信される（ステップ S 1 3 1 0）。

#### 【 0 1 4 2 】

図 1 4 は、本実施の形態のプリンタドライバ 1 2 1 0 で生成される印刷データの構造を示すデータ構造図である。図 1 4 に示すように、印刷データは、先頭にクライアント情報（I P アドレス）が付加されており、P J L 文書パスワード指定（暗号化）と P J L ジョブパスワード指定（暗号化）と暗号化 P D F 文書データ（暗号化）と P J L データ（暗号化）とから構成される。なお、P J L データは付加されていない場合もある。

#### 【 0 1 4 3 】

プリンタ装置 1 2 3 0 では、ホスト I / F 制御部 1 4 3 で印刷データを受信して（ステップ S 1 3 1 1）、復号化部 8 4 1 によって、鍵テーブルを参照し、受信した I P アドレスのクライアント情報に対応する公開鍵が有効であるか否かを判断する（ステップ S 1 3 1 2）。そして、有効である場合には、復号化部 5 4 2 によって秘密鍵で印刷データを復号化する（ステップ S 1 3 1 3）。そして、復号化された印刷データのデータ解釈処理を行い（ステップ S 1 3 1 4）、印刷データを H D D 1 4 9 に保存する（ステップ S 1 3 1 5）。ここで、データ解釈処理については実施の形態 1 のプリンタコントローラ 1 4 0 と同様の処理で行われる。一方、公開鍵が有効でない場合には、受信した印刷データを破棄し復号化処理を行わない（ステップ S 1 3 1 8）。

#### 【 0 1 4 4 】

図 1 5 は、H D D 1 4 9 に保存される印刷データのデータ構造図である。図 1 5 に示すように、印刷データは、ファイル名と描画データとジョブパスワードとユーザ I D と日付（ジョブ登録日付）とから構成され、ジョブパスワードとユーザ I D、さらにファイル名、日付から検索できるようになっている。

#### 【 0 1 4 5 】

次に、H D D 1 4 9 に保存される印刷データを選択するためのジョブ選択処理が行われる（ステップ S 1 3 1 6）。ジョブ選択処理では、まず、パネル制御部 1 4 4 が操作パネル 1 4 8 にジョブ選択画面を表示する。図 1 6 は、ジョブ選択



画面の流れの一例を示す説明図である。図 1 6 に示すように、ユーザ I D、ジョブパスワード、日付、ファイル名を入力することによって、蓄積制御部 1 4 5 は入力条件に合致する印刷ジョブの印刷データを H D D 1 4 9 から検索し、パネル制御部 1 4 4 によって、その内容を図 1 6 のジョブ一覧画面に表示する。

#### 【 0 1 4 6 】

ここで、ユーザ I D、ジョブパスワードを入力した場合には、そのユーザの全てのジョブがジョブ一覧画面に表示され、さらにファイル名、日付を入力することによって、そのユーザの全てのジョブの中で指定されたファイル名と日付に該当するジョブのみが検索されてジョブ一覧画面に表示されることになる。

#### 【 0 1 4 7 】

このジョブ一覧からユーザが所望のジョブを選択して O K ボタンをタッチ操作すると、選択されたジョブに対して、印刷制御部 1 4 6 によって印刷実行が行われる（ステップ S 1 3 1 7）。

#### 【 0 1 4 8 】

なお、本実施の形態のプリンタ装置 1 2 3 0 では、印刷データの H D D 1 4 9 への保存の処理（ステップ S 1 3 1 3）を、鍵の有効性の判断処理（ステップ S 1 3 1 2）の後に行っているが、P C 1 2 0 0 から印刷データを受信した時点で、H D D 1 4 9 に印刷データを保存し、その後、ジョブ選択処理を行って、鍵の有効性の判断処理を行うように構成しても良い。

#### 【 0 1 4 9 】

また、本実施の形態のプリンタ装置 1 2 3 0 では、印刷データの H D D 1 4 9 への保存の処理（ステップ S 1 3 1 3）を、データ解釈処理（ステップ S 1 3 1 4）の後、すなわち描画データへの展開後に行っているが、まずジョブの選択処理を行い、その後データ解釈処理を行うように構成しても良い。

#### 【 0 1 5 0 】

このように実施の形態 4 のプリンタドライバ 8 1 0 およびプリンタ装置 8 3 0 では、印刷ジョブを開始させるためのジョブパスワードを含む印刷データを生成して暗号化した上でプリンタ装置 1 2 3 0 に送信しているので、暗号化されたアプリ文書データの印刷時において、P D F 文書データを暗号化された状態のまま

、さらに印刷ジョブ毎に認証を行うことができ、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

#### 【0 1 5 1】

なお、本実施の形態のプリンタドライバ1 2 1 0では、ジョブパスワードをユーザに入力させることとしているが、文書パスワードが入力されたときに、ジョブパスワード処理部1 2 1 1によって文書パスワードからジョブパスワードを生成して用いるように構成してもよい。また、この場合、生成するジョブパスワードは、入力された文書パスワードと同一のものとすることも可能である。

#### 【0 1 5 2】

実施の形態1～4では、いずれもPDF文書データの印刷を例にあげて説明しているが、アプリケーション1 2 0によって暗号化される文書データであれば、PDF文書データに限らず、いずれの文書データにも本発明を適用することが可能である。

#### 【0 1 5 3】

また、実施の形態2～4には、PCのクライアント情報としてIPアドレスを使用しているが、例えば、装置固有識別番号等、PCを識別可能なデータであれば、いずれのデータもクライアント情報として使用することができる。

#### 【0 1 5 4】

##### 【発明の効果】

以上説明したように、請求項1にかかる発明によれば、暗号化されたアプリ文書データを復号化せずにプリンタ装置に送信して、同時に送信する文書認証情報によってプリンタ装置側で復号化して印刷を行えるので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを防止することができ、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データを暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

#### 【0 1 5 5】

また、請求項 2 にかかる発明によれば、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を第 2 の鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができ、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

#### 【 0 1 5 6 】

また、請求項 3 にかかる発明によれば、印刷ジョブごとに異なる第 1 の鍵情報を取得することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

#### 【 0 1 5 7 】

また、請求項 4 にかかる発明によれば、印刷する度に第 1 の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができるという効果を奏する。

#### 【 0 1 5 8 】

また、請求項 5 にかかる発明によれば、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を公開鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができ、また、プリンタ装置で秘密鍵情報を用いて復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

#### 【 0 1 5 9 】

また、請求項 6 にかかる発明によれば、印刷ジョブごとに異なる公開鍵情報を取得することができ、暗号化文書の印刷におけるセキュリティをより向上させる

ことができるという効果を奏する。

【0160】

また、請求項7にかかる発明によれば、印刷する度に第1の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができるという効果を奏する。

【0161】

また、請求項8にかかる発明によれば、暗号化されたアプリ文書データの印刷時において、アプリ文書データを暗号化された状態のまま、さらに印刷ジョブ毎に認証を行うことができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

【0162】

また、請求項9にかかる発明によれば、印刷ジョブ毎に認証に必要なジョブ認証情報を、アプリ文書データの暗号化に必要な文書認証情報から自動的に生成することができるので、ユーザに何度も認証情報を入力させる手間が省け、ユーザの便宜となるという効果を奏する。

【0163】

また、請求項10にかかる発明によれば、文書認証情報からジョブ認証情報を簡易に生成することができ、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させつつ迅速に行うことができるという効果を奏する。

【0164】

また、請求項11にかかる発明によれば、アプリ文書データを暗号化されたままクライアント装置から受信して、同時に送信する文書認証情報によってプリンタ装置側で復号化して印刷を行えるので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを防止することができ、また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データを暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

## 【 0 1 6 5 】

また、請求項 1 2 にかかる発明によれば、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を第 2 の鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができ、また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

## 【 0 1 6 6 】

また、請求項 1 3 にかかる発明によれば、要求された時点で直ちに印刷ジョブごとに異なる第 1 の鍵情報を送信することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

## 【 0 1 6 7 】

また、請求項 1 4 にかかる発明によれば、要求があった時点から印刷開始時までに時間差がある場合に、実際に印刷開始時に第 1 の鍵情報を送信することができるので、要求時点から印刷開始時点までの間に第三者が傍受することを回避することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

## 【 0 1 6 8 】

また、請求項 1 5 にかかる発明によれば、クライアント装置側で印刷する度に第 1 の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができるという効果を奏する。

## 【 0 1 6 9 】

また、請求項 1 6 にかかる発明によれば、第 1 の鍵情報の改ざんされた場合に暗号化されたアプリ文書データの印刷を未然に防止することができ、セキュリティの向上を図ることができるという効果を奏する。

## 【 0 1 7 0 】



また、請求項 1 7 にかかる発明によれば、アプリ文書データを暗号化された状態のまま、しかも復号化するための文書認証情報を公開鍵情報で暗号化された状態でクライアント装置から受信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができ、また、プリンタ装置で秘密鍵情報を用いて復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

#### 【 0 1 7 1 】

また、請求項 1 8 にかかる発明によれば、要求された時点で直ちに印刷ジョブごとに異なる公開鍵情報を送信することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

#### 【 0 1 7 2 】

また、請求項 1 9 にかかる発明によれば、要求があった時点から印刷開始時までに時間差がある場合に、実際に印刷開始時に公開鍵情報を送信することができるので、要求時点から印刷開始時点までの間に第三者が傍受することを回避することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

#### 【 0 1 7 3 】

また、請求項 2 0 にかかる発明によれば、クライアント装置側で印刷する度に公開鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができるという効果を奏する。

#### 【 0 1 7 4 】

また、請求項 2 1 にかかる発明によれば、有効期限切れで第三の傍受されたおそれのある秘密鍵情報によるアプリ文書データの復号化および印刷を防止することができ、セキュリティをより向上させることができるという効果を奏する。

#### 【 0 1 7 5 】

また、請求項 2 2 にかかる発明によれば、暗号化されたアプリ文書データの印刷時において、アプリ文書データを暗号化された状態のまま、さらに印刷ジョブ毎に認証を行うことができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

【図面の簡単な説明】

【図 1】

実施の形態 1 のクライアント装置（P C）およびプリンタ装置の機能的構成を示すブロック図である。

【図 2】

実施の形態 1 のプリンタドライバおよびプリンタ装置による暗号化 P D F 文書データの印刷処理の手順を示すフローチャートである。

【図 3】

実施の形態 1 の印刷データの解釈処理の手順を示すフローチャートである。

【図 4】

実施の形態 1 のプリンタドライバで生成される印刷データの構造を示すデータ構造図である。

【図 5】

実施の形態 2 のクライアント装置（P C）およびプリンタ装置の機能的構成を示すブロック図である。

【図 6】

実施の形態 2 のプリンタドライバおよびプリンタ装置による暗号化 P D F 文書データの印刷処理の手順を示すフローチャートである。

【図 7】

実施の形態 2 のプリンタドライバで生成される印刷データの構造を示すデータ構造図である。

【図 8】

実施の形態 3 のクライアント装置（P C）およびプリンタ装置の機能的構成を

示すブロック図である。

【図 9】

実施の形態 3 のプリンタドライバおよびプリンタ装置による暗号化 P D F 文書データの印刷処理の手順を示すフローチャートである。

【図 1 0】

実施の形態 3 の鍵テーブルのデータ構造図である。

【図 1 1】

実施の形態 3 のプリンタドライバで生成される印刷データの構造を示すデータ構造図である。

【図 1 2】

実施の形態 4 のクライアント装置（P C）およびプリンタ装置の機能的構成を示すブロック図である。

【図 1 3】

実施の形態 4 のプリンタドライバおよびプリンタ装置による暗号化 P D F 文書データの印刷処理の手順を示すフローチャートである。

【図 1 4】

実施の形態 4 のプリンタドライバで生成される印刷データの構造を示すデータ構造図である。

【図 1 5】

実施の形態 4 のプリンタ装置において H D D に保存される印刷データのデータ構造図である。

【図 1 6】

実施の形態 4 のプリンタ装置におけるジョブ選択画面の流れの一例を示す説明図である。

【図 1 7】

従来のプリンタドライバとプリンタ装置間を流れる印刷データの構造を示すデータ構造図である。

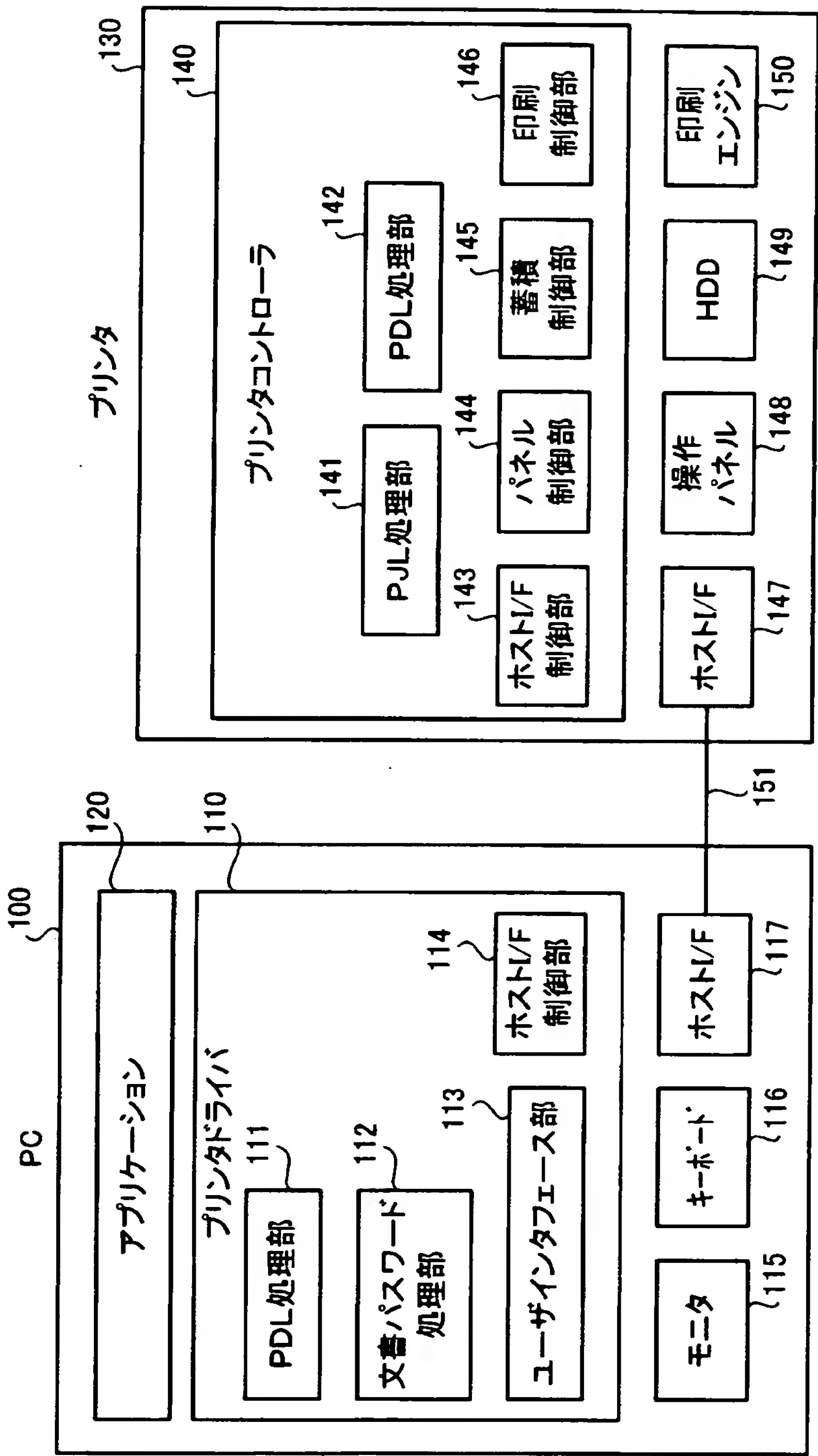
【符号の説明】

1 1 0, 5 1 0, 8 1 0, 1 2 1 0 プリンタドライバ

1 1 1, 1 2 1 2 P D L 処理部  
1 1 2 文書パスワード処理部  
1 1 3 ユーザインタフェース部  
1 1 5 モニタ  
1 1 6 キーボード  
1 2 0 アプリケーション  
1 3 0, 5 3 0, 8 3 0, 1 2 3 0 プリンタ装置  
1 4 0, 5 4 0, 8 4 0, 1 2 4 0 プリンタコントローラ  
1 4 1 P J L 処理部  
1 4 2 P D L 処理部  
1 4 4 パネル制御部  
1 4 5 蓄積制御部  
1 4 6 印刷制御部  
1 4 8 操作パネル  
1 4 9 H D D  
1 5 0 印刷エンジン  
5 1 1 S E E D 生成部  
5 1 2 暗号化部  
5 1 3 ジョブ制御部  
5 4 1 復号化部  
5 4 2 S E E D 元生成部  
8 1 2 暗号化部  
8 1 3 ジョブ制御部  
5 4 1, 8 4 1, 1 2 5 4 復号化部  
8 4 2 秘密鍵生成部  
8 4 3 公開鍵処理部  
1 2 1 1 ジョブパスワード処理部  
1 2 4 0 プリンタコントローラ

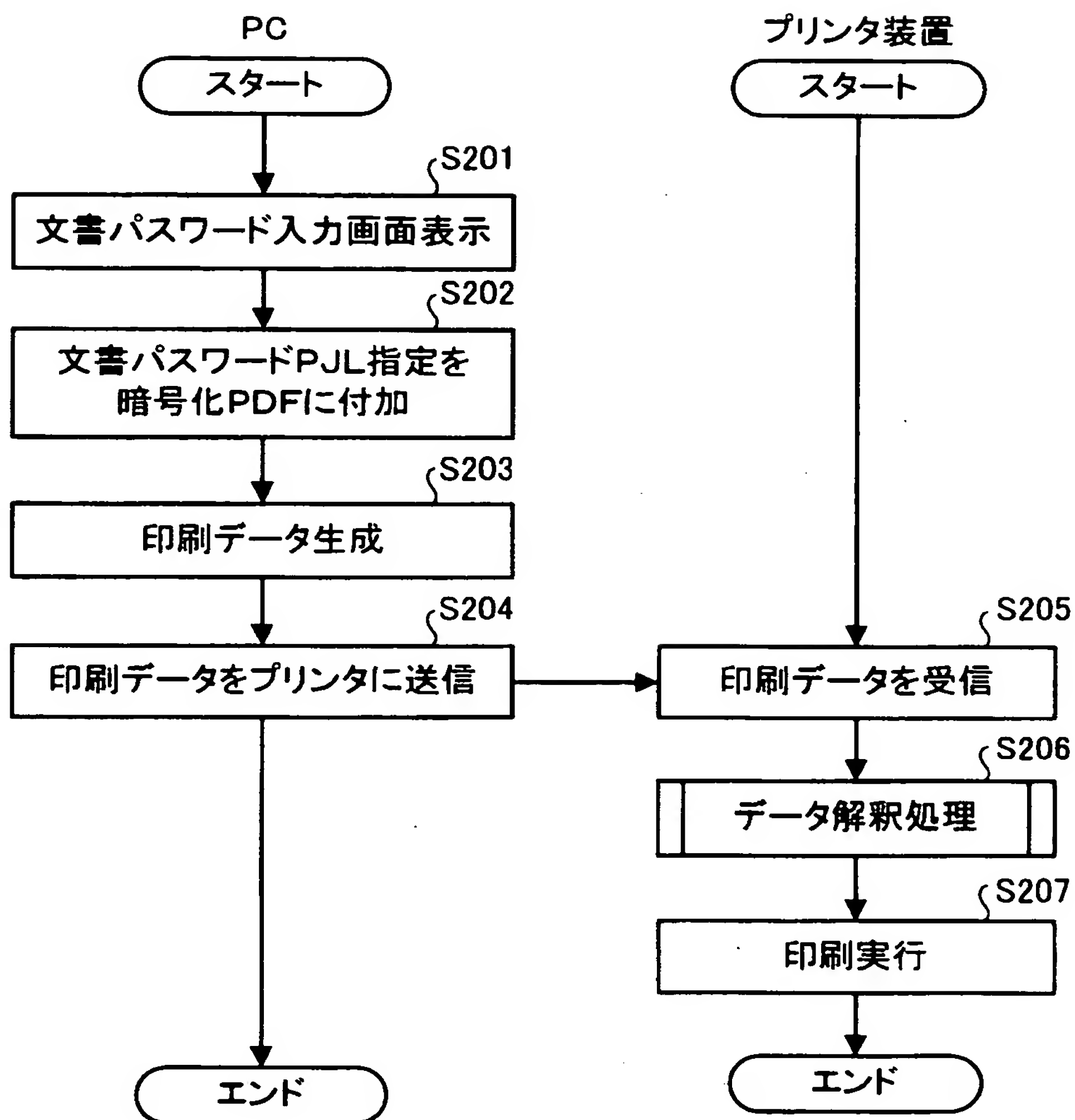
【書類名】 図面

【図 1】

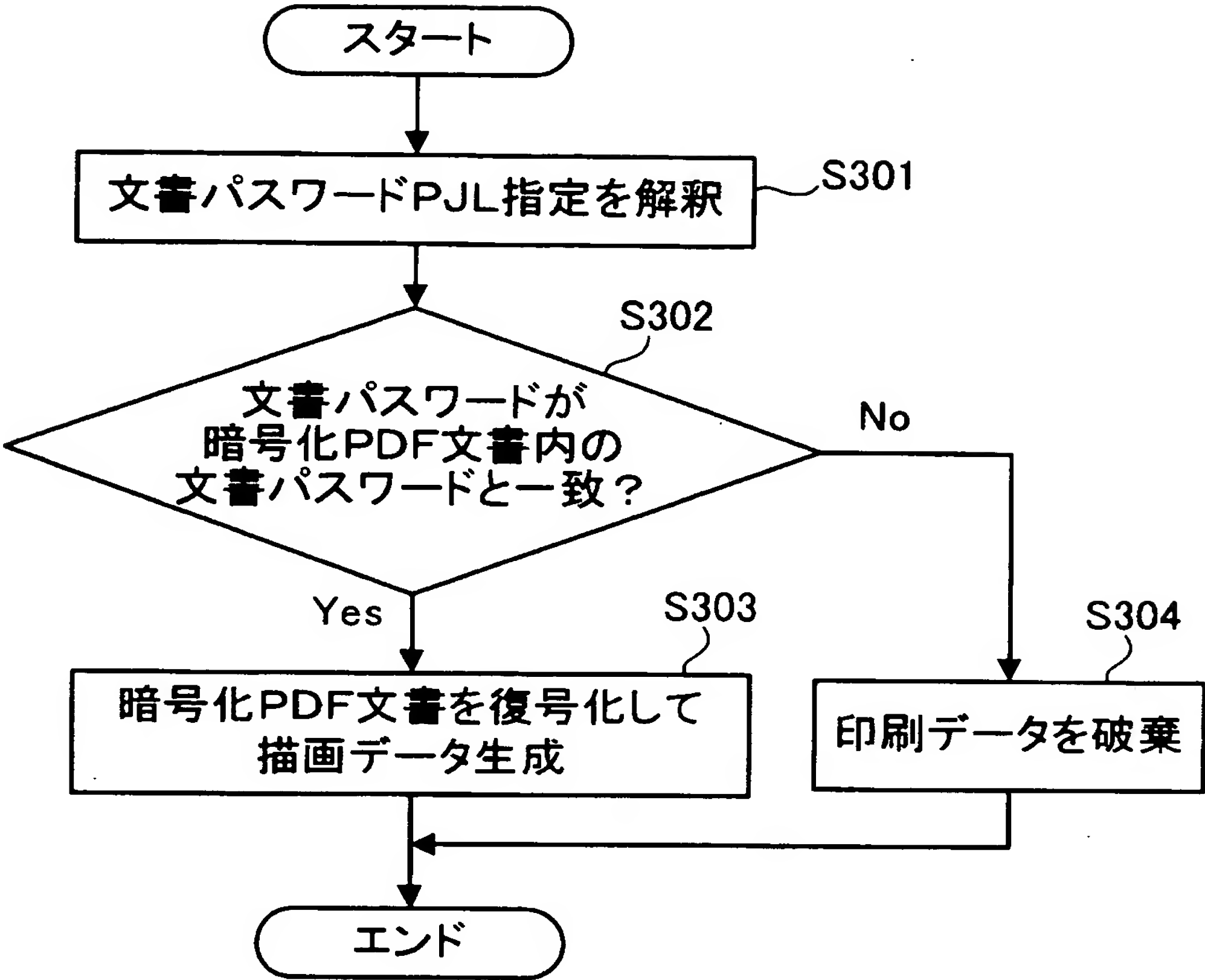




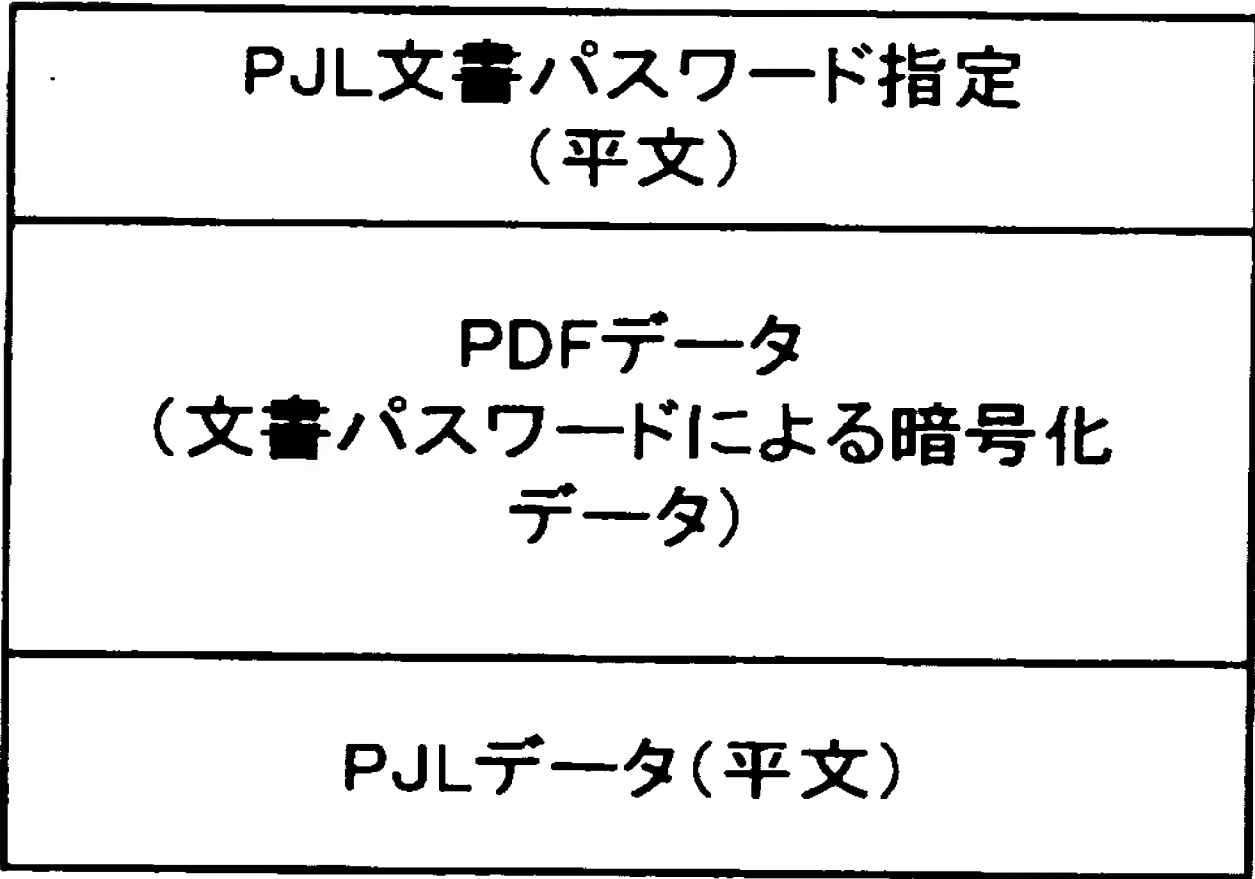
【図 2】



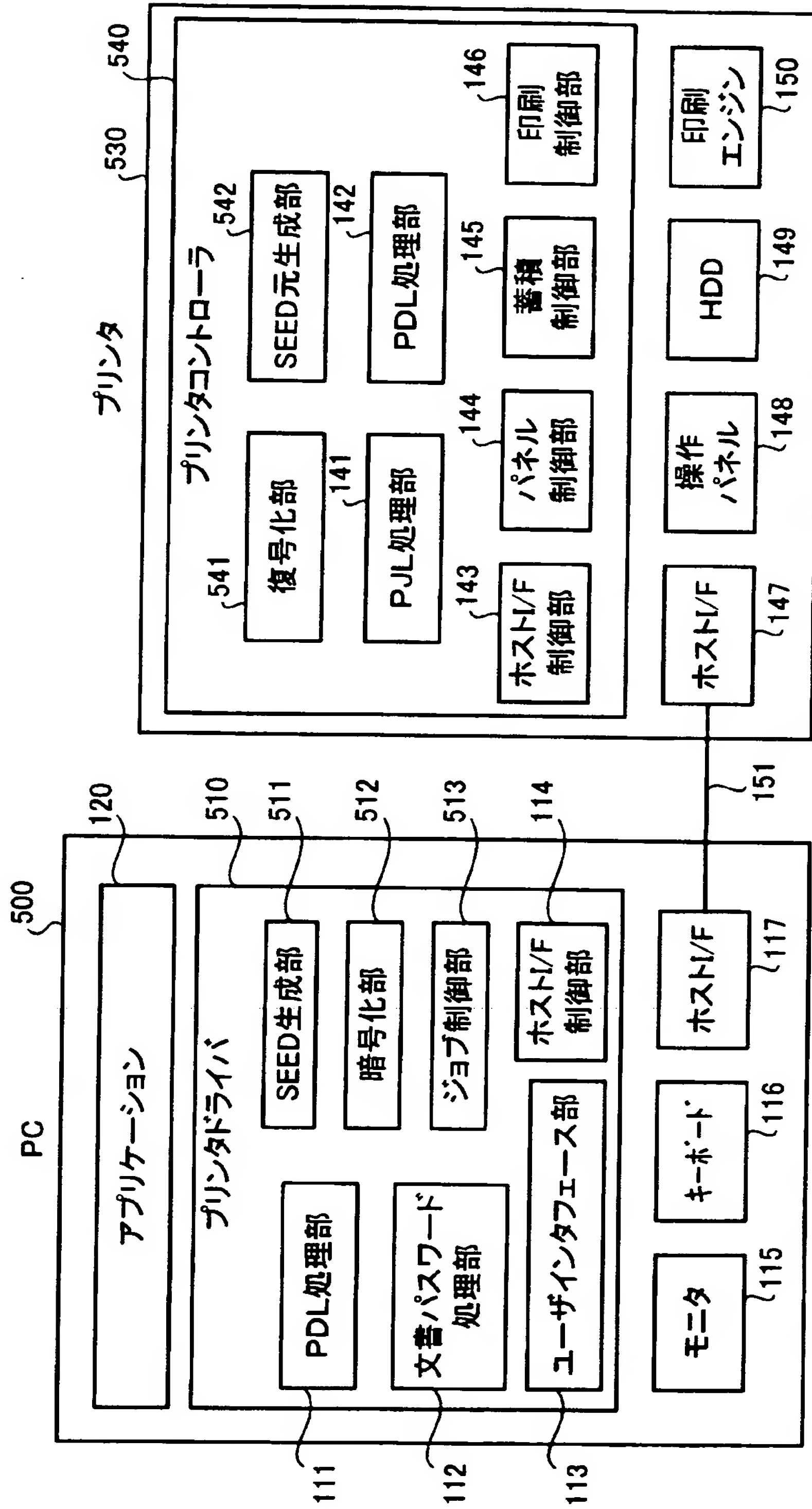
【図 3】



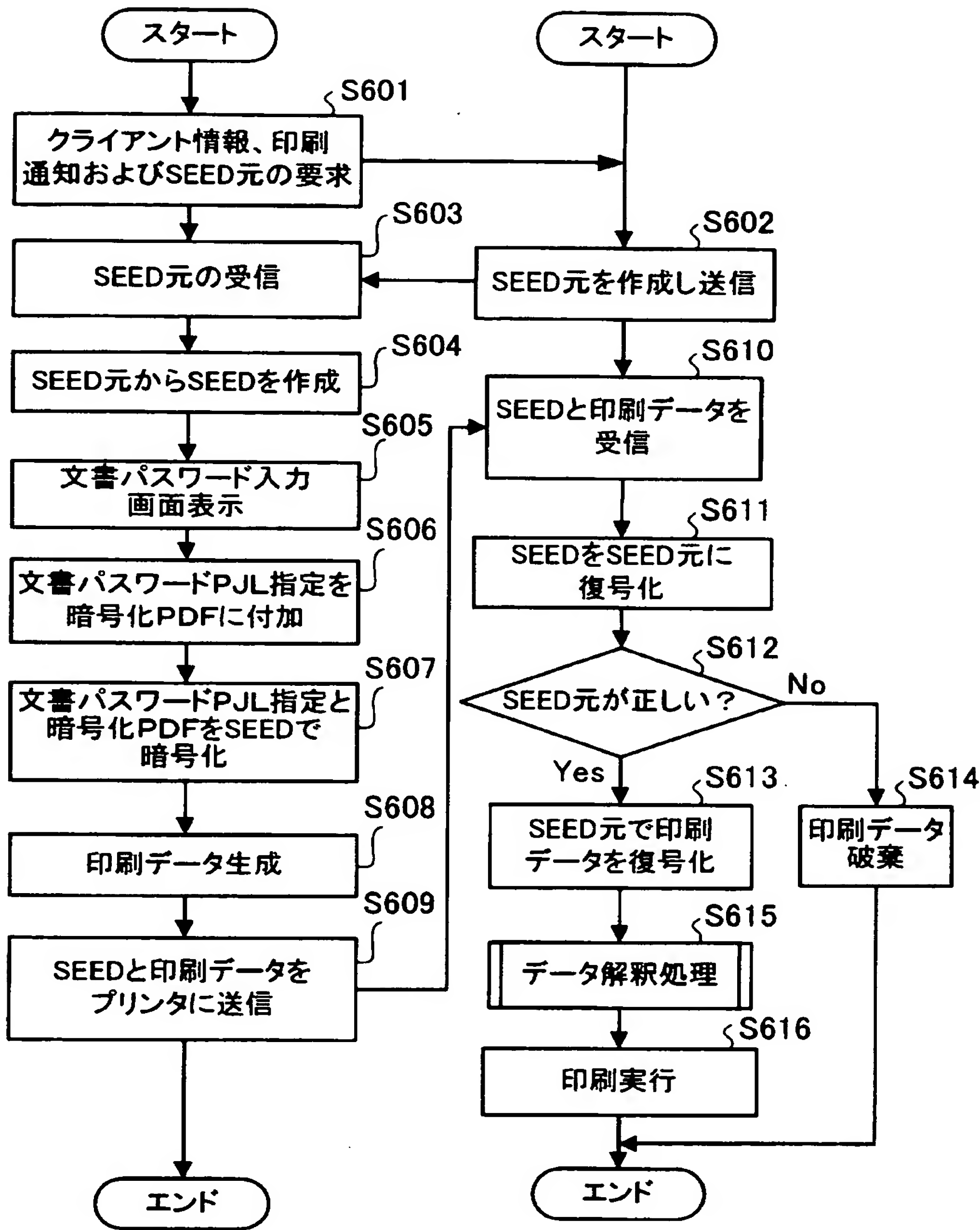
【図 4】



【図 5】



【図 6】

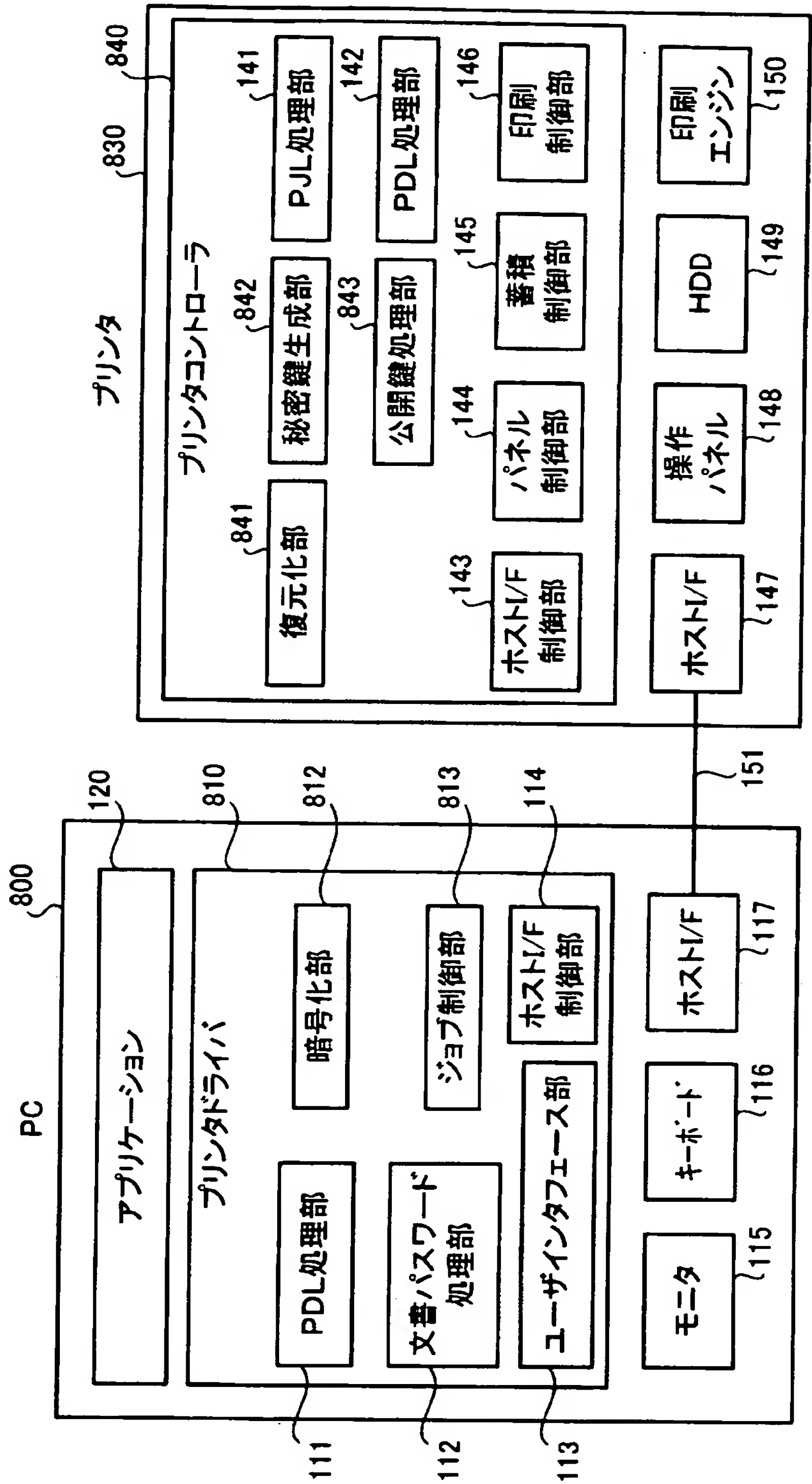


【図 7】

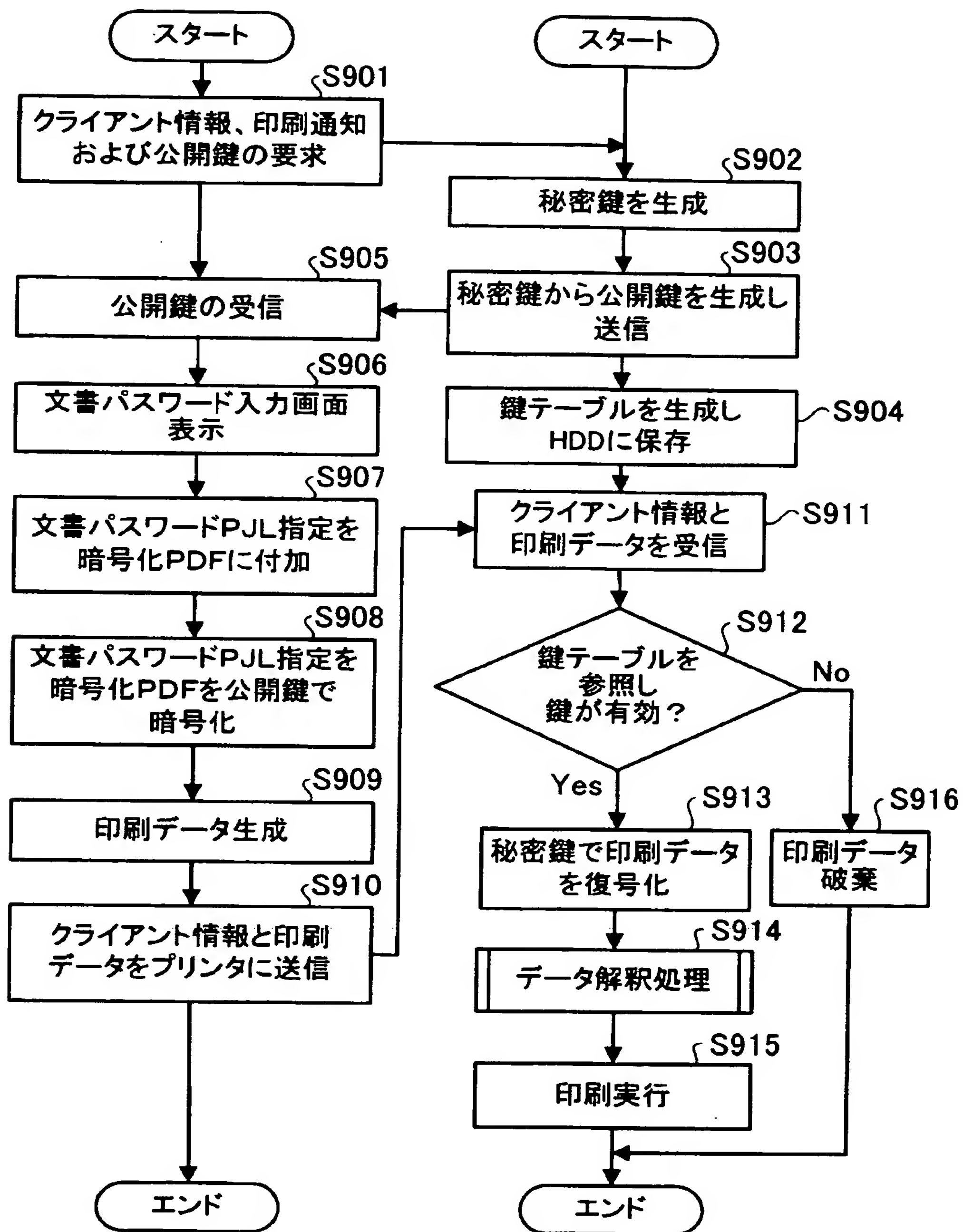
SEED
PJL文書パスワード指定 (SEEDにより暗号化)
PDFデータ (文書パスワードによる暗号化 データをSEEDにより暗号化)
PJLデータ(SEEDにより暗号化)



【図 8】



【図 9】



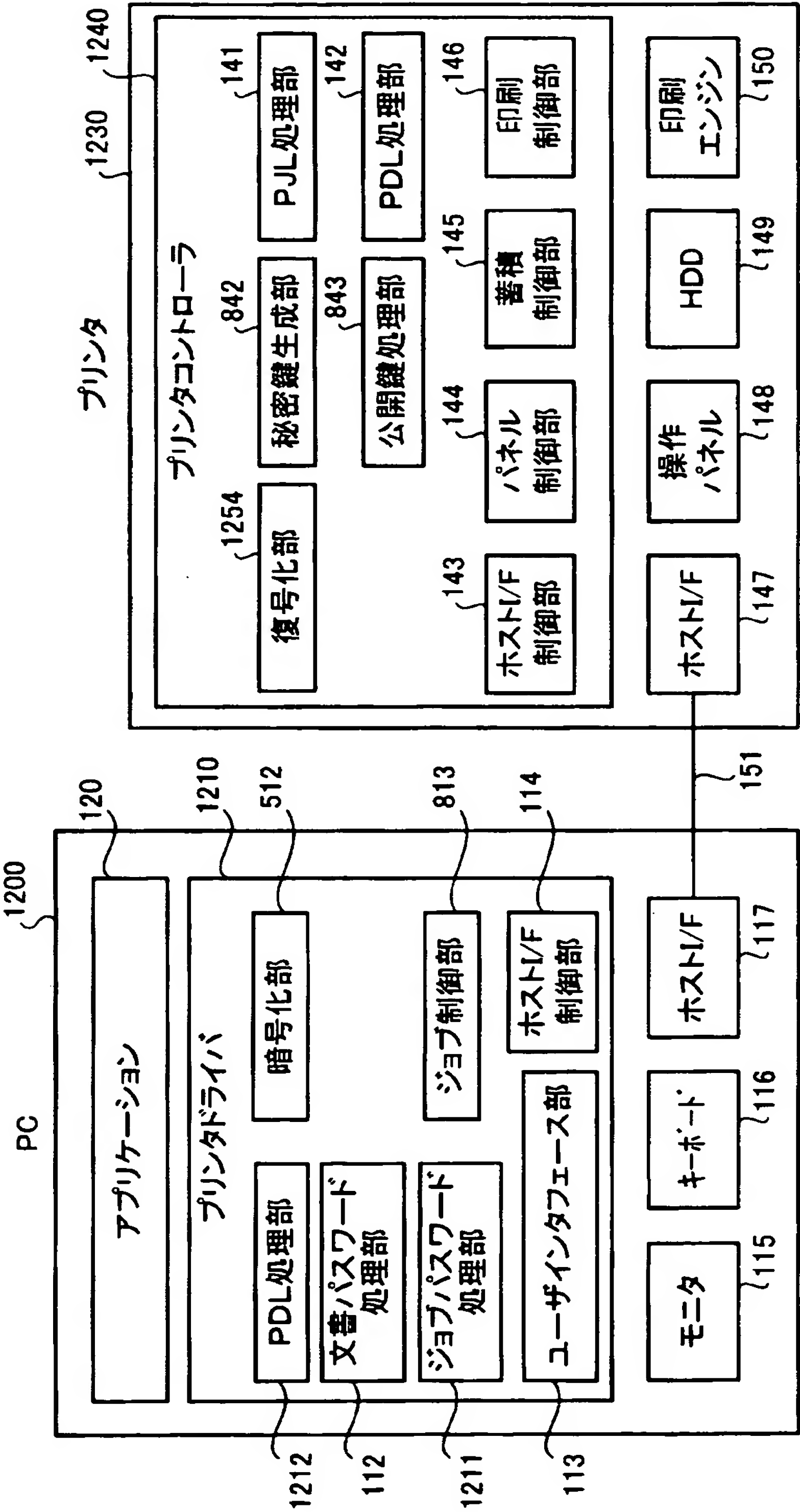
【図 1 0】

クライアント情報 (IPアドレス)	公開鍵	秘密鍵	有効期限
----------------------	-----	-----	------

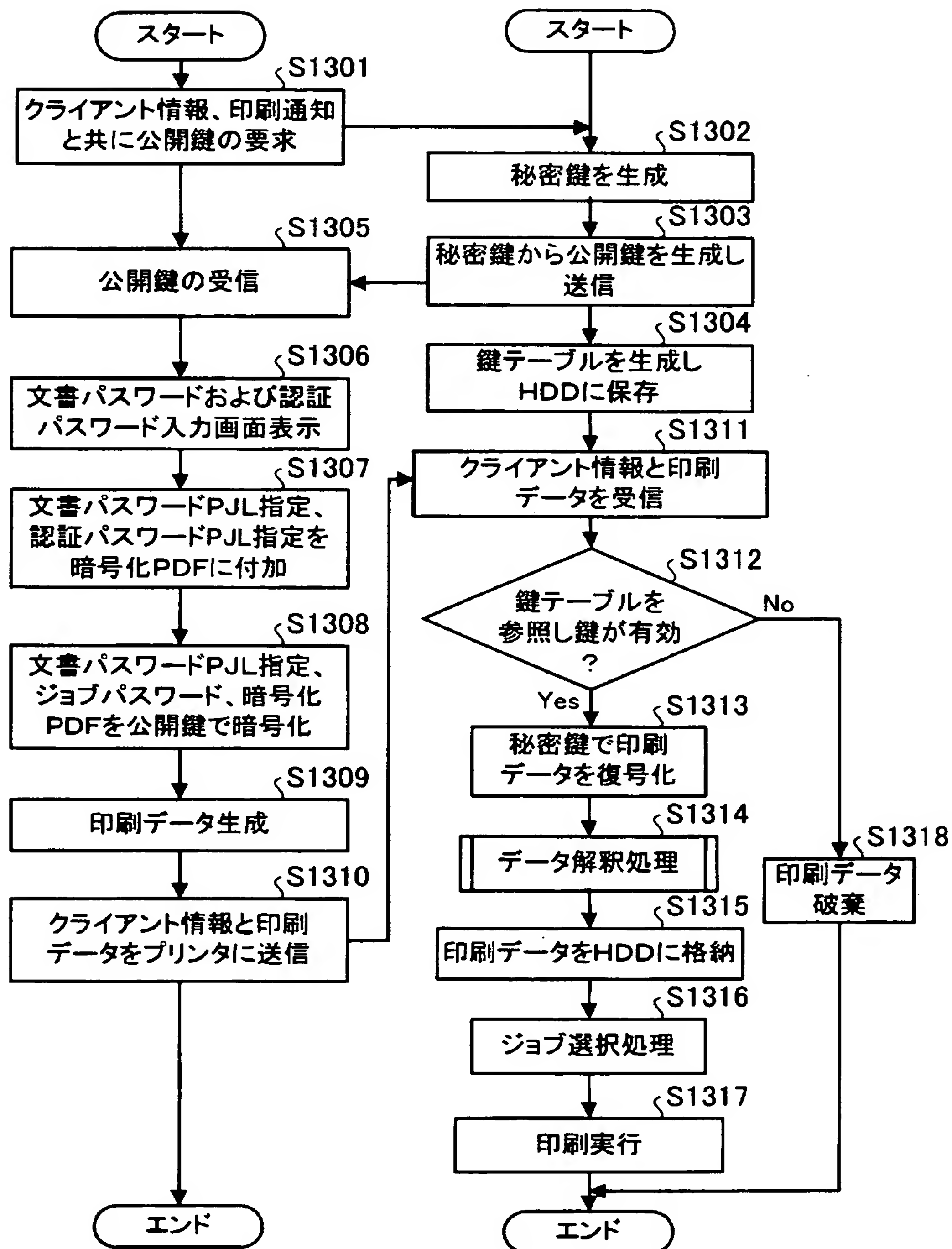
【図 1 1】

クライアント情報
PJL文書パスワード指定 (公開鍵による暗号化)
PDFデータ (文書パスワードによる暗号化データを 公開鍵による暗号化)
PJLデータ(公開鍵による暗号化)

【図 12】



【図 13】





【図 1 4】

クライアント情報
PJL文書パスワード指定 (公開鍵による暗号化) PJLジョブパスワード指定 (公開鍵による暗号化)
PDFデータ (文書パスワードによる暗号化データを 公開鍵による暗号化)
PJLデータ(公開鍵による暗号化)

【図 1 5】

ファイル名	描画データ	ジョブパスワード	ユーザID	日付
-------	-------	----------	-------	----

【図 1 6】

ユーザID:

ジョブパスワード:

日付(指定任意):

ファイル名(指定任意):

蓄積データ  
表示

OK

キャンセル

↓

ファイル名	日付
abc. doc	2002.12.11
123. xls	2002.02.05
...	...

蓄積データ  
表示

【図 1 7】

PJLジョブパスワード指定(平文)
PDFデータ(平文)
PJLデータ(平文)

【書類名】 要約書

【要約】

【課題】 アプリケーションで暗号化された文書データを印刷する場合においてもセキュリティを向上させること。

【解決手段】 ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラム 1 1 0 は、文書パスワード処理部 1 1 2 によって、アプリケーション 1 2 0 によって暗号化された P D F 文書データを復号化するための文書パスワードをユーザに入力させる。そして、暗号化された P D F 文書データと、文書パスワード処理部 1 1 2 によって入力された文書パスワードとを含む印刷データを生成する。そして、ホスト I / F 制御部 1 1 4 とホスト I / F 1 1 7 によって生成された印刷データをネットワーク 1 5 1 に接続されたプリンタ装置 1 3 0 に送信する。

【選択図】 図 1

特願 2 0 0 3 - 0 7 8 7 8 8

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 6 7 4 7 ]

1. 変更年月日

2 0 0 2 年 5 月 1 7 日

[変更理由]

住所変更

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー